INTELLIGENCE INFORMATION MANAGEMENT IN CRISIS SITUATION

Colonel drd. Dorin TOHANEAN
Ministerul Apărării

Abstract

The article aims to analyze the military information management in crisis situations. It includes all data and information from the security environment on which the optimum level of knowledge shall be ensured at the level policy-makers and politico-military status, of the system state parameters of the response system and the characteristics of the security environment from the areas of interest. The use of information is done for military training, substantiation and implementation of the decision of management factors, and for coordinating the implementation of the prevention measures for mitigation and crisis management.

I. Disasters prevention

Disasters are usually a result of organizations failing to prevent a crisis from getting worse, says Peter Power, Managing Director at Visor Consultants Limited. ‘There cannot be a crisis next week.

My schedule is already full’, said Henry Kissinger in June 1969 at a time when the US faced many potential crises. Humorous yes, but is there some truth in what he said? How many potential disasters are already on your corporate radar screen that you are too busy to notice? There you are, convinced that you have planned for just about everything. Your risk analysis is complete and all your information and data processing seems watertight. You are confident that

you are as prepared as you can be for most eventualities. Even the chairman has shown an interest. But what if fate delivers you a low ball and you have a crisis that really is out of the blue? How would you cope?

There is a worrying tendency, especially in the US, that assumes any 'out of the blue' crisis means just that: aircraft leaving the sky and deliberately hitting tall buildings – and we have all seen many post-9/11 business continuity plans that now focus exclusively on this threat to the exclusion of all others.

Whilst it is true that our notion of terrorism as a form of limited violence was shattered by the terrible events in 2001, previous attacks by equally less predictable terrorist organizations – like the Aum sect in Japan, responsible for the Tokyo subway nerve gas attack and fanatical groups in the Middle East – had already challenged our previous assumptions about terrorism. It was, and will always be, a threat that is surprisingly hard to define.

Almost by definition, terrorism will continually seek to change its face. But enough has already been written on this subject and before we also slide towards overindulging our concern with just one type of threat, let us return to the subject of this article: **can you really handle any crisis?**

My own belief is that crisis prevention is considerably more effective than disaster recovery, but many organizations are encouraged by some consultants to spend a disproportionate amount of time and money on recovery options, without first looking at reducing risks, as well as preparing for the unforeseen.

II. Containing a crisis is more effective than recovering from a disaster.

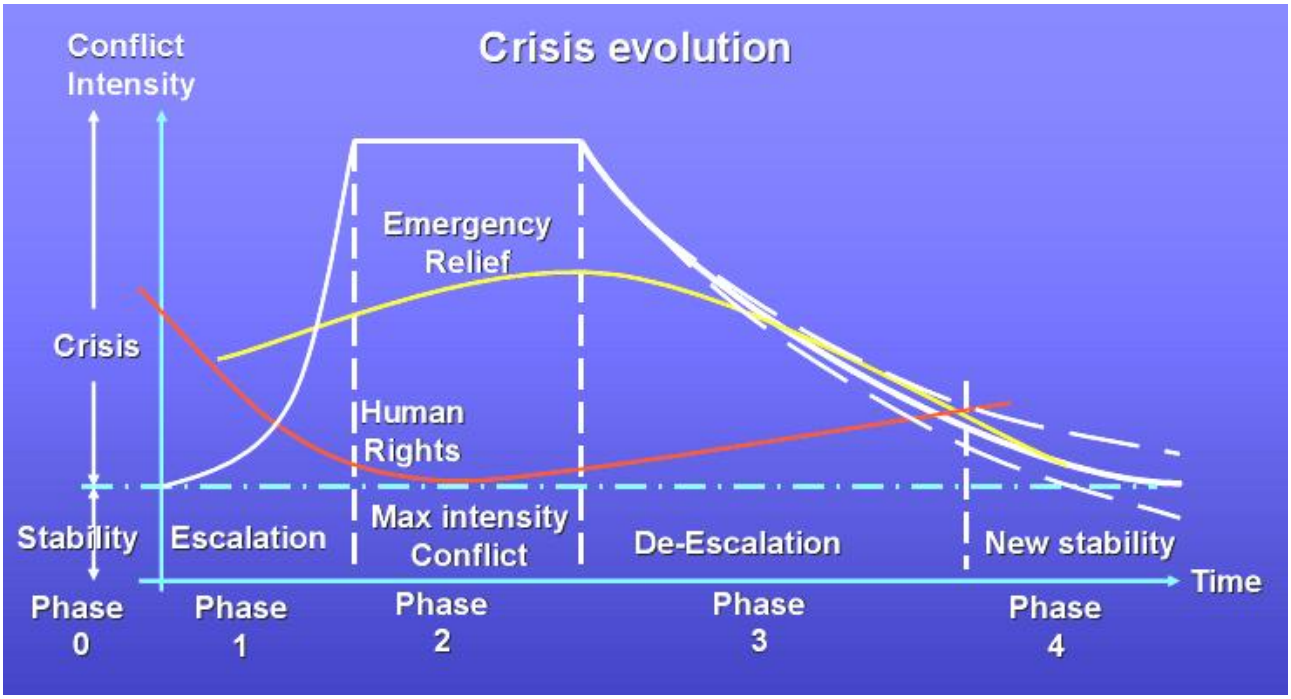

Figure 1 Crisis evolution

Manage your risks properly and recognize that the key to successful crisis management is to realize that containing a crisis is more effective than recovering from a disaster. Oddly enough, many organizations have disaster recovery plans, but not enough have crisis management options. Perhaps that is because you can more easily measure recovery? This leads to the last point: When setting up any measurement criteria, seek out what is important and then work out how to measure it (for example, measuring the likely damage to reputation).

At the beginning of the **Vietnam War**, the US Army had numerous fire-fights with the Vietnamese Army and quickly realized that the number of enemy dead invariably far exceeded their own. This was easy to measure and thus could be used to calculate who would win the war, and how soon. However, in doing this the US Army, like many before it, made the mistake of finding **something to measure** and then making it important, rather than the other way around.

For the Vietnamese Army, leaving the dead in the field was irrelevant when you had endless reserves, control over domestic media coverage and a will

to win. The truth is that almost all crises follow a path from normality to possible disaster.

Crisis management can recognize and interrupt this if applied diligently and on time. In the case of a bomb explosion without warning, this path will be sudden; but such a scenario is an exception, as many incidents can be termed ‘quiet catastrophes’ that build up, often unnoticed (small errors that are not checked soon become big problems).

This can include scenarios such as power failure, intermittent system faults, road closures, sabotage, protestors, corrupt data, or building-related issues such as faulty air conditioning. Sometimes organizations have first been alerted to a crisis because the press called to tell them – in which case they might already be halfway down the path to disaster where trying to take the ‘media high ground’ is even more imperative. Indeed, the issue of presentation and media image is so important that we have seen some companies ultimately fail even though their efforts on site were as good as they could be, but they somehow failed to give the right message to the world’s media.

When speaking to the press, try and avoid the five ‘d’s:

- **d**enying everything;
- **d**oing nothing;
- **d**iverting to someone else;
- **d**iminishing the incident;
- **d**rip-feeding at your own pace.

It is often the case that organizations have not necessarily taken the wrong actions in terms of crisis management but probably took the right ones too late – by which time the crisis itself sets the pace and you might end up following events rather than getting in front and stopping the spread.

By calculating an assessment of the crisis situation and its likely development – coupled with what should be the ideal reaction to control, contain and resolve it – it is possible to draw a basic model to illustrate the point that

few crises instantly jump from normality to disaster. It is therefore possible to assess the impact of the crisis and its likely rise/fall, and then link this directly to the best reaction to contain it, to reassure stakeholders, and so on. In this way a crisis management structure can quickly be set up, but populated only according to present and anticipated requirements. For example, there is a 'stage 1' crisis that puts some people on standby whilst others are engaged in 'fire fighting'. Subsequently, the incident can be either downgraded or upgraded to a 'stage 2' crisis, where levels may be fully staffed on a shift basis. The outline structure, however, remains the same. But setting all this out in a few pages may ignore a particularly vital feature. Unfortunately, too many crisis planners often overlook human emotion.

Too many practitioners see the processes they are dealing with as highly systematic, cerebral and conscious: you know what you are doing and you can explain the process to others. Emotion is seen as something that clutters up the calm processing of information and is nearly always factored out of the equation. That is one reason why my own company specializes in crisis management, since when your own schedule is full and human emotion is ignored you can be sure that a crisis is soon to follow.

II.1 Chains of evidence

Contrary to popular perception, most e-business and information security crimes and abuses that are reported today are internally inspired and range from theft of information to sabotage. As a result, the work of the computer forensics expert is a far more complex operation than most people appreciate. Computer forensics enables the systematic and careful identification of evidence in computer-related crime and abuse cases. This may range from tracing the tracks of a hacker through an organization's IT systems, to tracing the originator of apparently anonymous defamatory emails, to recovering evidence of fraud. But, as with any investigation, it is vital to know where to look to find the evidence

required and how not to destroy that very evidence in the process. This requires skill, knowledge and a lot of experience – especially as all forensic investigations must respect the laws governing the rights of the individual in each country and must always be handled with sensitivity. A computer forensics investigation can reveal practically everything, from the character of the user, to their interests, activities, financial health, acquaintances and more. It is all there to be recovered from applications, email systems, Internet browsers and free space. Their life, outlook, intelligence and interactions are held – as individual as any fingerprint – on the computer they use.

There is no limit to the accountability that can be uncovered: private business transactions, communications with accomplices, fraud indicators and much more are frequently mined from systems. Attempts to hide or erase this evidence are often unsuccessful, and a 'golden nugget' that proves a crime can be unearthed by an expert. The evidence that a forensics investigation will seek to uncover will vary; but activity such as Internet abuse during working hours is a good example of a well-known business problem. Amongst the more prevalent cases tend to be problems involving employees who divulge critical corporate information to third parties, fraud and the diversion of sales to rival companies for generous kickbacks. Cases of anonymous harassment and defamation are increasing along with the use of email and the Internet, and hacking cases involving Trojan horses, denial of service attacks and network intrusions also feature highly in the typical forensics workload.

Industrial espionage is also still a problem, and the discovery of 'key loggers' is increasing with improved user awareness. A small hardware device or software utility such as this can easily be installed and go unnoticed. These simple tools can help a competitor or criminal to steal passwords and user IDs in an instant. Without the correct security procedures, the victim won't know a thing about it until it's too late. But it is not only employees that forensics investigations focus on. So few companies have adequate security vetting

procedures, that industrial espionage has become a global concern. Every computer, on practically every desk, is an open doorway to the company's network and all of its data and essential information, such as its payroll, projects, R&D, finance, patents and customer details. Everything is potentially there for the taking by professionals posing as cleaners, tradesmen, maintenance crews, fitters and even, sometimes, as clients. Cases of arson have been brought to trial using computer forensic techniques, and bandwidth problems in large corporations have been found to be a result of network abuse by personnel downloading massive video files (sometimes full-length, hi-resolution feature films), MP3 music files, or simply spending all day listening to global radio over the Internet. Petty jealousy is also an increasing problem in many organizations: better cars, larger offices, fatter salaries and unpopular promotions can provoke the worst kind of unreasonable behavior. The result is that sabotage is a growing problem, with people systematically and knowingly breaking systems.

II.2 Gathering the evidence

The process of gathering evidence requires proper incident management training. Investigators must follow the correct procedures or the evidence may be compromised and become inadmissible. Simply booting a PC will change at least 70 of its parameters. In addition, documentation of the steps taken in a forensic investigation is vital, and a case can be built on suspicious activity. Why does the suspect work so often at weekends? Why does he/she never take leave? Is there a regular pattern of people who always work long hours, often late into the evening? The ideal is to take copies of the entire hard drives of the suspect systems for examination with forensic software, but this is not always possible and a strict procedure for identifying and securing potential evidence is required.

There is also an array of pitfalls to be avoided when attempting to secure reliable evidence: it must not be damaged, destroyed or compromised in any way, and steps must be taken to ensure that the investigation:

- does not change any of the time and date stamps of files;
- does not change the contents of the data itself;
- maintains a complete and comprehensive audit trail of the steps taken;
- understands what operations the computer performs when it is turned on or off.

Computer forensics is a growing area that is earning increasingly wider recognition; and as systems and networks increase in complexity, it is becoming more and more specialized. It is also the area for specialist companies who have the resources, knowledge and experience to really make a difference. There is a growing awareness of the requirements for handling computer evidence in the country due to an established and accepted code of practice and the number of cases passing through the Courts. However, the chain of evidence is frequently not confined to one country and may cover many different countries and several continents, requiring forensic specialists to understand international law. It is also important to remember that it is only possible to uncover what is actually there. This may seem like an obvious point to make, but computer forensics cannot promise or perform miracles, and the most obvious pieces of evidence, such as a letter written to an accomplice, logging dates, times and transactions, found in the free space on a disk is a highly unusual occurrence.

A really good forensics team can tell, in an instant, whether a business has good grounds for further investigation or not. They will know from their initial examination whether something looks wrong and out of place. Such a decision can often save a company many thousands of pounds and a lot of wasted time. As the discipline develops, forensics is spreading into whole new areas. Specialist teams are not only being tasked with handling criminal incidents but also with developing and implementing blocking, prevention and tracking

techniques in companies and throughout organizations. But the fact is that most hacking cases are not pursued as far as they should be – companies simply rebuild their systems and get on with business, due to fear of the expense and loss of time that prosecution might involve. Forensic specialists are increasingly advising on the viability of potential courses of action, and are increasingly being called upon to help pinpoint sources of danger and devise procedures that prevent repeat attacks. Theft of company information and intellectual property is still the largest area of corporate crime, and computer forensics is certain to grow in importance as the volume of e-commerce transactions increases and as access to company networks and corporate information needs to be more reliably protected and ever-more tightly controlled.

II.3 Challenge for intelligence in the market state

The United States will face some fearsome snakes, some of which will be closed to view and so require old world methods. Yet the dominant feature of the new world is how much information is out there. Intelligence is no longer just in the secrets business, it is in the information business. The implications of the shift are dramatic. The explosion of information means that policy officials will be more, not less, reliant on information brokers. If collection is easier, selection will be harder. There will also be more brokers and more competition among them.

Intelligence analysts will be one set of brokers, but others, the competition, will range from CNN, to Bloomberg and Oxford Analytic, to journalists and academics.

The more open world is blurring the distinction between collection and analysis. The best looker is not a spy-master, much less an impersonal satellite, but someone steeped in the substance at hand - in short, an analyst. Yet analysts now get rewarded for being generalists, not deep specialists, and in some areas, such as economics, intelligence cannot compete with the private sector.

Analysts, though, are cheap in comparison with satellites, and hiring more people from outside, even for brief tours, would deepen the intelligence community's expertise.

In the circumstances of the high Cold War, there were powerful arguments for targeting intelligence tightly on the Soviet Union; for giving pride of place to secrets, especially those collected by satellites and other technical means; for centralizing intelligence; and for separating it from the stakes of policy agencies. None of these arguments, however, is compelling today.

With one target and one preeminent consumer - in form the President but in fact the National Security Council, encompassing the State and Defense departments and the NSC staff - there was a certain logic to the way intelligence was, and is, organized. It was structured according to the different ways intelligence is collected - the National Security Agency for intercepting signals; SIGINT, the CIA's clandestine service, for spying; HUMINT; and so on. These "INTs," or "stovepipes" in the language of insiders, could each concentrate on the distinct contribution it could make to understanding the Soviet Union. In the process, though, those "INTs" became formidable baronies in their own right.

Now, however, the old structure just has to be wrong. No business would organize this way. Now, there are many targets and many consumers, though there are some consistent alignments among targets, customers and collectors. In these circumstances, a firm would organize by lines of business, establishing a distributed network or a loose confederation in which different parts of intelligence would endeavor to build very close links to the customers each served. The existing Director of Central Intelligence centers - for counterterrorism, counternarcotics, and the like - are suggestive models. They do organize by problem or line of policy. They primarily integrate within the world of intelligence, though they provide a focal point for connecting to policy. And the distributed network would be "virtual," not bricks and mortar, because

while some problems, such as North Korea or terrorism, will be enduring, others will rise and recede quickly.

In a world of too much information, policy-makers will want to "pull" up what they need, not have information "pushed" upon them; they will want to pull up puzzle solutions when they need them, not receive a torrent of information whether they ask for it or not. Yet solving the puzzle is often important enough that getting policy officials to pay attention is not a problem.

Mysteries are more abundant now, and the franchise of framing strategic mysteries is very different from solving puzzles. Analysts need access to secrets, but their crucial partnerships are those with colleagues outside intelligence and outside government, in the academic and think-tank worlds, in nongovernmental organizations and in private business. Intelligence needs to be opened wide, not cosseted in secret compartments. This franchise is based on the recognition that intelligence's business is information, not secrets, and that its product is experts, not paper.

In a world where both structures and U.S. interests are up for grabs, policy-makers would be better served by intelligence brokers close at hand, down the hall, not out at Langley. Perhaps the CIA should be dispersed, its analytic pieces assigned to the State, Treasury and Commerce departments and elsewhere across official Washington.

The last part of the challenge for intelligence in the market state will be to reach out to new partners, especially in dealing with hard targets such as terrorism. It will mean conceiving of intelligence strategically, as a means of helping others see a set of issues the way the United States does and so facilitating the building of coalitions. While U.S. intelligence has been creative, in fact, in sharing intelligence - for instance, in U.N. peacekeeping operations - in principle, sharing has been a grudging act, letting a few trusted friends see some of the crown jewels if they had something to contribute in return. Building relationships will still be an important reason for sharing, but in the future, the

partners will be much more varied - not just intelligence agencies but NGOs, not just foreign offices but foreign companies. And the sharing will be two-way, not one. In the world of the market state, a world that is not fully open everywhere but is not very closed anywhere, humanitarian NGOs will know more about many African countries than the CIA, and oil companies will be just as expert on Indonesia.

The market state ultimately will invoke the dilemma of how much intelligence can be broadened to serve shared international purposes, given its very national origins. After all, intelligence has been thought of as the way to get a leg up on other nations, not bring them into coalitions of the willing. The campaign against terrorism, for instance, will bring together the willing and the reluctant. Countries and groups that are no friends of the United States may be brought into an anti-terrorism coalition, and intelligence cooperation - including laying out the case against particular terrorists - will be part and parcel of assembling and sustaining such a coalition. In time, the coalition might give real force to an international norm against terrorism.

But in the process, virtually all the distinctions on which U.S. intelligence has been based would be strained. Intelligence and law enforcement would be forced together. Distinctions between "home" and "abroad" would be hard to sustain as terrorist networks reach across borders and even include American citizens. U.S. collaborators would run well beyond trusted friends, to those who are neither friends nor states. Finally, the intensity of cooperation required would leave the intelligence community hard-pressed not to reveal something of its capacity, if not its sources and methods.

III. Supporting Elements for NATO Crisis Management

The NATO Crisis Response System (NCRS), the NATO Intelligence and Warning System (NIWS), NATO's Operational Planning System and NATO Civil Emergency Planning Crisis Management Arrangements are designed to

underpin the Alliance's crisis management role and response capability in a complementary and synergistic fashion, as part of an overall NATO Crisis Management Process.

The practices and procedures which are used form the Alliance's crisis management arrangements. Facilities, including communications, in support of the process are provided by the NATO Situation Centre (SITCEN), which operates on a permanent 24-hour basis. Exercises to test and develop crisis management procedures are held at regular intervals in conjunction with national capitals and NATO Strategic Commanders. Crisis management arrangements, procedures and facilities, as well as the preparation and conduct of crisis management exercises, are coordinated by the Council Operations and Exercise Committee (COEC), which also coordinates crisis management activities with Partner countries.

The Council Operations Section supports NATO crisis management by the development and improvement of procedures, organization and facilities to support the needs of the Council and Defence Planning Committee, and to facilitate consultation in periods of tension and crisis.

The Peacekeeping Section supports the crisis management process by providing conceptual and technical strategic planning and advice on peace-support operations. The Peacekeeping Staff also support other aspects of NATO's work in the field of crisis response operations, including the development of Alliance peacekeeping policy, the development of CIMIC (Civil-Military Cooperation) policy, and support for the NATO-Russia Council (NRC) and Political Military Steering Committees (PMSC) Ad Hoc Groups on Peacekeeping. This section also maintains close relations with other international organizations including the OSCE and UN.

The Situation Centre, known as the SITCEN, has three specific roles:

- to assist the North Atlantic Council, the Defence Planning Committee and the Military Committee in fulfilling their respective

functions in the field of consultation;

- to serve as a focal point within the Alliance for the receipt, exchange, and dissemination of political, military, and economic intelligence and information;
- to act as a link with similar facilities of member nations and of the major NATO Commands.

III.1 A Communication Centre or "COMCEN" supports the Situation Centre.

At the earliest opportunity, the Partners and then non-Partner nations are invited and consulted to offer forces. These contributions are often in important areas of Allied shortfall such as medical, engineering and technical specialists. The intention behind participation by Non-NATO Troops Contributing Nations (NNTCN) is to create a truly multinational framework and to better demonstrate international support and **legitimacy**. The NNTCN are also given the opportunity to comment on operations planes, and their views are taken into account. This allows partner and non-partner nations to contribute to the provision of political guidance and oversight of operations, and contributes to what is called as "Decision Shaping".

Non-NATO Nations close to the conflict area can also offer Host Nation Support in the form of basing, transit and over-flight rights. This kind of support is, in many situations, crucial.

In response to a potential or developing crisis, to acting on time it is essential to have a variety of different measures or possible responses in place, so that they do not have to be developed on an ad-hoc basis for each new situation. In deciding what to do about a given situation, the Council/DPC has a wide range of measures, and Allies have agreed from which to choose. These measures have been substantially revised since the end of the Cold War to seek to ensure that they are relevant for the contemporary crisis environment.

Measures include:

(1) diplomatic, economic and military preventive measures,

(2) a large variety of military response options and

(3) a spectrum of precautionary measures.

Examples of the preventive measures could include: messages, trade restrictions, expressions of support for threatened states, closure of ports and airports and special programs in favor of threatened states. Examples of military response options could include: cancellation of military cooperation, confidential military consultations, request inspections and evaluation visits, surveillance, increased readiness and activation of forces. There are also a variety of contingency operation plans, which can be drawn on for detailed operational planning if required.

In addition to these lists of measures, NATO also has a system for assuring preparedness and timely response in crisis for civil and military commands, agencies and headquarters, and national military units and agencies.

IV. Indicators of Romanian Armed Forces strategy for cyber security and information intelligence

Romanian Armed Forces have already prepared the National Crises Response System (Figure no. 2).

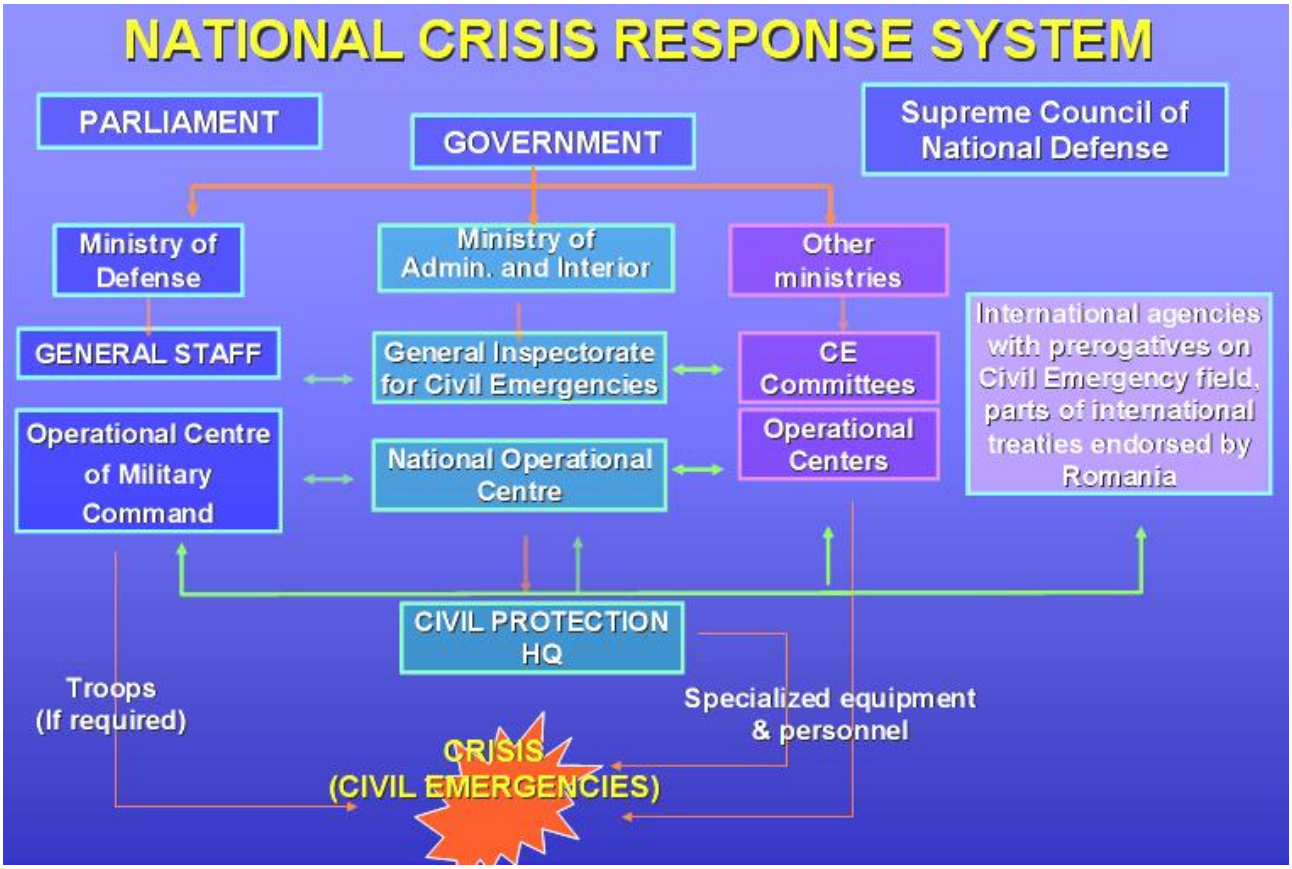

Figure no. 2 The National Crises Response System

Romanian Armed Forces strategy for cyber security and information intelligence could be founded on sound principles and technologies, including and not limited to these indicators:

- Better precision in understanding existing and emerging vulnerabilities and threats;
- Advances in insider threat detection, deterrence, mitigation and elimination;
- Game-changing ventures, innovations and conundrums (e.g., quantum computing, QKD, phishing, malware market, botnet/DOS);
- Assuring security, survivability and dependability of our critical infrastructures;
- Assuring the availability of time-critical scaleable secure systems, information provenance and security with privacy;

- Observable/ measurable/ certifiable security claims, rather than hypothesized causes;
- Methods that enable us to specify security requirements, formulate security claims, and certify security properties;
- Assurance against known and unknown (though perhaps pre-modeled) threats;
- Mission fulfillment, whether or not security violations have taken place (rather than chasing all violations indiscriminately).

Conclusions

In the circumstances of an age of information, perhaps it is time for intelligence to "split the franchise" and dramatically change how it is organized. Today's tactical puzzles where secrets matter are both fewer and more varied than the Cold War's Soviet puzzles, but they are still important. For solving puzzles, analysts need to be close to the collectors of secrets.

We must shift our focus away from winning battles, towards a strategy for winning the war by elevating trust in the mission and it's underlying critical infrastructures.

REFERENCES

1. NATO Handbook, NATO Office of Information and Press, 2001; http://www.nato.int/docu/handbook/2001/index.htm

2. Atran, Scott. “The Moral Logic and Growth of Suicide Terrorism.”The Washington Quarterly 29,no.2 (Spring 2006):127-147. A study of the different views on the causes of suicide terrorism.

3. Bjorgo, Tore,ed.The Root Causes of Terrorism: Myths,Reality and Ways Forward.London:Routledge, 2005.

4. Richard et al. A Blueprint for Action New York:Century Foundation,2004.

Clark Defeating the Jihadists: A detailed analysis of the different terrorist groups that have been spawned by Al Qaeda and are now part of analyzed terrorist network.

5. Cronin,Audrey Kurth. “How al-Qaida Ends: The Decline and Demise of Terrorist Groups. ”International Security 31,no.1 (Summer 2006):7-48.

6. Kohlman, Evan. “The Real Online Terrorist Threat.”Foreign Affairs 85,no.5 (Sept./Oct.2006):115-125.

7.http://ec.europa.eu/justice_home/fsj/terrorism/strategies/fsj_terrorism_strategies_counter_en.htm.