Early-Warning. A "Threat" for Extremism

drd. Aitana BOGDAN
National Intelligence Academy *"Mihai Viteazul"*
aibogdan@dcti.ro

Motto: *"It is pardonable to be defeated, but never to be surprised"*
Frederick the Great

Abstract:

The intelligence field is currently undergoing a structural reform and transformation process, which is broadly entitled by experts as a revolution in intelligence affairs (RIA). Among various other changes, we also encounter an increased concern for finding novel instruments of processing information, which can be employed by intelligence organizations for preventing emerging risks and threats.

This paper focuses on one such tool, namely early-warning systems and tries to asses whether it would prove an efficient instrument in preventing extremist actions. Additionally, the study attempts to identify the main advantages and disadvantages of developing such a system inside an intelligence organization both from the point of view of information accuracy and of human and logistic resources deployed.

Keywords: early-warning, OSINT, SWOT, extremism, methodology

1. Definition and typology:

There is no unique definition for early-warning, as the concept has transformed and gained multiple meanings in accordance with the domain in which it was applied. Initially the concept of "early-warning" was developed during the Cold War in the field of military intelligence to enhance the capacity of predicting potential ballistic attacks[1].

Afterwards, the United Nations used early-warning as an instrument

[1] Niels von Keyserlingk and Simone Kopfmüller, *"Conflict Early Warning Systems. Lessons Learned from Establishing a Conflict Early Warning and Response Mechanism (CEWARN) in the Horn of Africa"*, October 2006 available at http://www.gtz.de/de/dokumente/en-igad-Conflict-Early-Warning-Systems-Lessons-Learned.pdf, accessed on 02.03.2012.

to forecast natural disaster, defining it as *"the provision of timely and effective information, through identified institutions, that allows individuals exposed to hazard to take action to avoid or reduce their risk and prepare for effective response"*[2].

Nevertheless, early-warning can be found in various other fields such as crisis management, economy, education and intelligence. For example, in business intelligence, EW is defined as *"an organized, systematic approach to intelligence gathering and analysis that allows companies spot threats and opportunities more quickly than their competition."*[3]

While there is no unique definition of the concept, most experts in the field agree that any early-warning system, independent of the field in which it is developed must include four main components[4]:

1. **risk knowledge**: risk assessment provides essential information needed to set priorities for mitigation and prevention strategies and designing early-warning systems

2. **monitoring and predicting**: EWS need monitoring and predicting capabilities to provide timely estimates of the potential risk

3. **disseminating information**: communication systems are need for delivering warning messages to the selected beneficiaries (be they public or private entities). The message needs to be reliable, synthetic and simple.

4. **response**: coordination, good governance and appropriate action plans are needed.

Failure of any part of the system will imply failure of the whole system. Every early-warning system is, thus based on a trade-off between timelines, warning reliability, the cost of a false alert and damage avoided as a function of lead time, which must be modeled to determine the cost efficiency of the outcome[5].

The tolerable threshold for a false alarm decreases as the cost of action increases or when the cost savings due to mitigation decrease. Because shorter time scale forecasts are, in general, more reliable, the

[2] Veronica S. Grasso, Ashbindu Singh, *Early Warning Systems: State-of-Art Analysis and Future Directions* available at http://na.unep.net/geas/docs/Early_Warning_System_Report.pdf, accessed on 02.03.2012.

[3] Kenneth Sawka, *The Intelligence Edge*, p. 21-22, July 2005 available at http://www.outwardinsights.com/articles/Leadership-Reprint-lowres.pdf accessed on 02.03.2012.

[4] Veronica S. Grasso, Ashbindu Singh, *op. cit.* accessed on 02.03.2012.

[5] David Rogers and Vladimir Tsirkunov, "Costs and Benefits of Early Warning Systems", *Global Assessment Report on Disaster Risk Reduction*, 2010 available at http://www.preventionweb.net/english/hyogo/gar/2011/en/bgdocs/Rogers_&_Tsirkunov_2011.pdf, accessed on 02.03.2012.

probability of a false alarm decreases as the lead time for the predicted onset of the crisis/hazard decreases. However, the shorter lead time also means reduced cost savings due to less damage avoided[6].

Although there are many variations in the structure of existing early-warning system, an ideal structure should resemble the following model[7]:

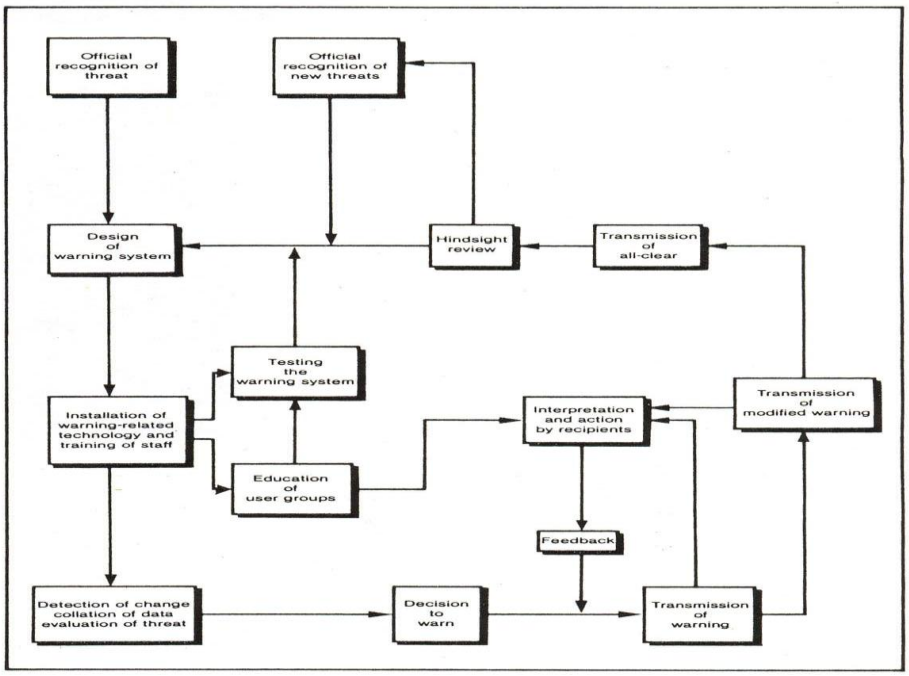

Fig. 1 – Structure of an Early Warning System (Foster, 1980)

Most early-warning system are based on open source information (OSINT), which allow the detection of weak signals regarding the possibility of a negative event occurring. Between 80% and 90% of the necessary information can be gathered through open sources.[8]

From the point of view of intelligence services, early-warning systems may prove to be a useful tool as they assist these organizations in performing one of their most fundamental functions – anticipation and prevention

[6] *Ibidem*.

[7] Michael H. Glantz, *Usable Science 8: Early Warning Systems: Do's and Don'ts*, October 2003, p. 15 available at http://ccb.colorado.edu/warning/docs/report.pdf, accessed on 02.03.212.

[8] Lucia Montaro and Julia Schünemann, *Walk the Talk: The EU Needs an Effective Early Warning System to Match Its Ambitions to Prevent Conflict and Promote Peace*, February 2011 available at http://www.ifp-ew.eu/pdf/walkthetalk.pdf, accessed on 02.03.2012.

of security risks and threats, in short it insures surprise avoidance.

In the last decades the development of early-warning systems has greatly evolved that is why we can now distinguish between different generations of EWS. First generation systems, created in 1990s are focused on analysis and often have a mandate that is about promoting evidence-based responses to crisis in the institutions they serve. Second-generation systems have appeared in 2000s combine analysis and advocacy in the attempt to catalyze responses of external institutions, while third-generation systems (developed post-2003) integrate early-warning and early response together[9].

From a broader perspective, EWS can be classified in: (1) pro-active, in which an organization first determines which are its priorities and then goes about monitoring those issues and (2) reactive, in which an organization uses early-warning as a radar looking for unexpected changes[10].

2. General benefits of Early Warning Systems

The first and foremost benefit acquired by any type of organization after implementing such a system is an increase in the time resource needed in the process of preparing, analyzing and planning a response to a crisis. This is turn leads to an increase in the likelihood of success. Early-warning can also be used in the planning process, contributing to the establishment of goals and the development of courses of action[11].

Among the most successful early-warning systems are FEWER (Forum on Early Warning and Response), Strategic Intelligence developed by Shell International, GOARN (Global Outbreak and Alert Response Network) and HEWS (Humanitarian Early Warning Service).

3. General Disadvantages of Early Warning Systems

Criticism of EWS ranges from the system's inability to predict crises beyond the obvious trends to their lack of synchronization with the interests, capacities and institutional constraints of the end user[12].

---

[9] David Nyheim, *The Global Balance Sheet: Emerging Security Threats and Multilateral Response Capabilities*, The Stanley Foundation, October 2009, p. 3 available at http://www.stanleyfoundation.org/spc_2009/Nyheim.pdf, accessed on 02.03.2012.

[10] Allesandro Comai, *Early Warning Systems For Your Competitive Landscape*, Society of Competitive Intelligence Professionals, vol. 10, no. 3, 2007, pp. 7-11.

[11] John Kriendler, "Anticipating crises", *NATO Review*, Winter 2002 available at http://www.nato.int/docu/review/2002/issue4/english/art4.html, accessed on 02.03.2012.

[12] Anna Matveeva, *Early Warning and Early Response: Conceptual and Empirical Dilemmas*,

One of the most cited problems is that in many cases early-warning does not lead to timely, relevant and effective action from the part of the authorities, a problem generally described as the *"warning-response gap"*[13].

This is connected both with the cognitive biases related to risk and threat perception of decision-makers and the manner in which open sources are perceived in comparison to other intelligence sources[14].

Among the biases identified in policymakers' response are *"loss aversion"*[15] and *"aversion to certain losses"*[16], *"extension neglect"*[17] and *"psychic numbing"*[18].

Moreover, a significant number of decision makers continue to consider OSINT as being unreliable and are as such unwilling to take important decisions based on such intelligence products.

The last and most important disadvantage of early-warning systems is their consumption of large financial and human resources. Even the best and most sophisticated system will not work efficiently without the necessary financial and human resources and substantial investment in professional training[19].

In the last years, the quantity of available open source information has increased considerably, which makes the process of turning it into OSINT very costly, time-consuming, requiring also specific skills, money and methodology.

4. Importance of Anticipation and Early Warning for Intelligence Organizations

After the end of the Cold War we have witnessed a multiplication and diversification of risks and threats to security. Therefore, the institutions, which have a mission to provide intelligence to decision – makers must face a very specific challenge: they must focus on developing

---

Issue Paper 1, September 2006 available at http://www.gppac.net/uploads/File/Resources/GPPAC%20Issue%20papers/Issue%20paper%201.pdf, accessed on 02.03.2012.

[13] Lucia Montaro and Julia Schünemann, *op. cit.*, accessed on 02.03.2012.

[14] *Ibidem.*

[15] Loss aversion means that people prefer the status quo over a 50/50 chance for positive and negative alternatives with the same absolute value.

[16] People prefer to avoid a certain loss in favor of a potential loss, even if they risk loosing significantly more.

[17] People tend to give an action the same value to an action regardless of the number of units it will affect.

[18] People have difficulties in processing and responding to harm affecting large numbers of people.

[19] Lucia Montaro and Julia Schünemann, *op. cit.*, accessed on 02.03.2012.

the capabilities and organization of intelligence with the aim of trying to understand this evolving multidimensional security.

If organizations are to fulfill this task, they must start by grasping the nature of the relation between national security, public policies and intelligence. According to Dennis Blair in his Statement before the Senate Select Committee on Intelligence *"nothing is more important to national security and the making and conduct of good policy than timely, accurate and relevant intelligence… The Intelligence Community is charged with the task of assessing threats and providing timely warning"*[20].

The importance of anticipation and foresight is stressed in most documents concerning the objectives and activities of intelligence organizations. For example, the French 2008 White Paper emphasizes the importance to *"know and anticipate"*, while a CIA document states *"reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us – the prelude to decision and action by U. S. policymakers"*[21].

In Romania, the National Defense Strategy of 2010, a strategic document, albeit never adopted mentions among the objectives of the Intelligence Community, the need to "improve its early-warning capabilities regarding events, which may prove dangerous for Romania"[22].

Therefore, we can conclude that a fully developed and integrated capacity for foresight, long-range analysis or anticipation and warning should be an integrated part of the intelligence activity.

Here, we should make a distinction between strategic warning (the fact that some negative event may take place) and tactical warning (short time regarding the time and place of that event). Intelligence and early-warning can function at both these levels, although early-warning systems generally focus only on strategic warning[23].

---

[20] Statement of Dennis C. Blair before the Senate Select Committee on Intelligence, 22 January 2009, apud Helene Lavoix, *Enabling Security for the 21st Century: Intelligence & Strategic Foresight and Warning*, 2 August 2010, available at http://www.rsis.edu.sg/publications/WorkingPapers/WP207.pdf, accessed on 02.03.2012.

[21] Central Intelligence Agency, *A Consumer's Guide to Intelligence,* Washington DC, 1999, p. vii apud Helene Lavoix, *op. cit.*, accessed in 02.03.2012.

[22] *National Defense Strategy*, 2010, p. 24, available at http://www.presidency.ro/static/ordine/SNAp/SNAp.pdf, accessed on 20.02.2012.

[23] Michael Hough, "Warning Intelligence and Early Warning With Specific Reference to the African Context", *Strategic Review for Southern Africa*, November 1st 2004, available at http://goliath.ecnext.com/coms2/gi_0199-4363882/Warning-intelligence-and-early-arning.html,

Furthermore, we should be aware of the fact that early-warning differs from intelligence systems in several ways. Firstly, unlike intelligence systems, an early-warning system does not focus on threats to itself, but it is concerned with the protection of the population of a certain state[24]. Secondly, a warning cycle is complete only after the decision-maker has been warned and a decision has been taken. This is why, in comparison to intelligence systems, early-warning implies a close linkage between analysis and action, objectivity being preserved through the transparent nature of the EWS[25].

Niels von Keyserlingk and Simone Kopfmüller provide a comparison on the differences between intelligence and early-warning in general terms[26].

	Intelligence Services	Early Warning Systems
Approach	Interventionist	Facilitative
Method	Quantitative	Qualitative
Goal	Prediction	Anticipation
Formulation	Universal Laws	Context
Results	Universal Patterns	Dynamic
Concerns	Strategic Security	Human Security
Information Base	Secret	Transparent
Institutional Base	Centralized	Decentralized

While intelligence systems rely mainly on secrecy, early-warning uses transparent methods and depends on the sharing of information, even though these exchanges and the communication of results may be classified and restricted to different categories of users[27].

Nevertheless, early-warning information must fulfill the same standards of accuracy, validity, reliability, timeliness and verifiability as intelligence products[28].

5. Generating Early Warning for Extremism

accessed on 02.03.2012.

[24] *Ibidem.*

[25] Jackie Ciliers, "Towards a Continental Early Warning System for Africa", *ISS Paper 102*, April 2005, p. 2 available at http://www.iss.co.za/pubs/papers/102/Paper102.htm, accessed on 02.03.2012.

[26] Niels von Keyserlingk and Simone Kopfmüller, *op. cit.*, accessed on 02.03.2012.

[27] *Ibidem.*

[28] *Ibidem.*

The greatest difficulty in developing an early-warning system for extremism is related to the formulation of critical indicators.

By definition, a critical indicator is a *"significant clue about what is happening and the eventual end state of a series of events. To fulfill their intended functions, critical indicators must be defined so that they occur early in the evolution of the crisis in such a way that, if identified decision-makers have time to react"*. They also have to be reliable so as to convince policy-makers to base their actions on them. As a general trait, indicators must be collectable and identifiable to allow a EWS to detect them if they exist[29].

This can represent a significant problem if we are to take into consideration there is no unique understanding of the meanings of the concept "extremism".

This difficulty can be overcome by extrapolating certain indicators used in early-warning systems for terrorism or conflicts. For example, Massimo Fusato's classification of variables for early-warning signs of conflict can successfully be employed with certain modifications in developing a qualitative analysis tool for a EWS for extremism[30]. The resulting categories would be the following:

a. demographic
   - demographic changes (especially of minorities)
   - increasing territoriality of peoples
b. economic
   - economic/financial crisis
   - short-term and long-term changes in economic performance of a country
   - increase in poverty/inequality
   - rise of unemployment rate
c. policy related
   - active discrimination or legislation favoring one group over another
   - potentially destabilizing referendums or elections
d. public opinion or social factors
   - rise in societal intolerance or prejudice
   - increase in number of demonstration and rallies

[29] John Kriendler, *op. cit.*, accessed on 02.03.2012.
[30] Massimo Fusato, *Preventive Diplomacy and International Violence Prevention*, October 2003 available at http://www.beyondintractability.org/node/2742, accessed on 05.03.2012.

e. external
- intervention or support on behalf of one of the parties/groups by an external actor
- "diffusion" or "contagion" of extremist ideologies in neighboring countries
- influx of extremist sympathizers from other countries

Based on this methodology a three-stage analysis process should be put into place. The first consists in collecting and analyzing data on the perceived threat – individual, group, event or activity. The second stage studies the national context in search of vulnerabilities, triggers or deterrents in respect to the perceived threat. The third and final stage combines the finding of the first two stages to generate a comprehensive risk assessment. A research cycle is complete when the level of threat is satisfactorily assessed.

6. SWOT Analysis

SWOT Analysis *on the development of an early-warning system for extremist activity by a Romanian intelligence organization*

Internal	**Strengths** • experience in OSINT collection[31] • possession of necessary technology for OSINT collection[32] • existence of communication channels with governmental institutions • experience in dealing with extremist threat[33]	**Weaknesses** • requires important financial and logistic resource • lack of personnel with experience in the development and management of EWS • difficulties in formulating critical indicators for extremist activity • image loss if warnings prove inaccurate

[31] www.sri.ro/categorii/56/centrul-surse-deschise.html, accessed on 02.03.2012.
[32] *Ibid*.
[33] www.sri.ro/categorii/22/apararea-constitutiei.html, accessed on 02.03.2012.

External	**Opportunities** • European Union has interest in and funds development of EWS • working EWS on terrorism in other states • the importance of anticipation function for intelligence organizations is mentioned in a security strategic document • ample literature available on the subject of EWS development	**Threats** • Difficult economic climate • Strong criticism from civil society if the warnings prove inaccurate • Lack of awareness at national level of importance of EWS for insuring security • Poor relations between intelligence organizations, the academic community and the private sector

		Strenghts				Weaknesses				Total
Opportunities		1	2	3	4	1	2	3	4	
	1	0	0	0	0	1	1	0	0	2
	2	0	0	0	0	0	0	1	0	1
	3	0	0	0	0	0	1	0	0	1
	4	0	0	0	0	0	1	1	0	2
Threats	1	0	1	0	0	1	1	0	0	3
	2	0	0	1	0	0	0	0	1	2
	3	0	0	1	0	0	0	0	1	2
	4	0	0	1	0	0	0	0	0	1
Total		1	1	3	0	3	4	2	2	

The analysis of the SWOT matrix reveals the importance of the following items which have received a score of at least 3 points:

- Strength 3 – existence of communication channels with governmental institutions
- Weakness 1 – requires important financial and logistic resource
- Weakness 2 – lack of personnel with experience in the development and management of EWS
- Threat 1 – difficult economic climate

These results are an indicator of what should be the key-concerns for a Romanian intelligence organization in the process of developing an early-warning system for extremism.

The most critical issue appears to be insuring the necessary

resources, both financial and human needed for the development of an early-warning system. From this point of view an intelligence organizations benefits from a certain advantage, as it already possesses OSINT specialists as well as intelligence analysts. The difficulty appears in adapting the working procedures and methodology so as to fit those of a EWS, while preserving the confidentiality and security protocols in place. Moreover, Romanian intelligence organizations have little experience with the development and management of early-warning systems, thus needing to resort to outside experts in the field.

On the long run, this could prove an advantage as it may build the foundation for establishing a fruitful partnership between intelligence organizations, the academic community and the private sector, which is the main requirement for building an intelligence culture.

The financial dimension of the problem can be addressed by identifying grants and outside donors. For example, the European Union funds research projects aimed at developing early-warning systems in various fields such as conflict prevention, economic threats, diseases, illegal substances etc.

In what concerns the communication channels with the beneficiaries, Romanian intelligence organization should capitalize their experience in improving analyst-decision maker relations and intelligence feed-back systems in order to overcome the warning-response gap. While a direct linkage between the intelligence analysis unit and the policy-makers, as mentioned in all early-warning methodologies is not possible according to the current security procedures, a possible solution could be the creation of the so-called "trusted networks", which would enable better cooperation and collaboration between the two sides.

7. Conclusions

On the short and long term there is a need to increase the understanding of the added value of early-warning. Education and training programs on how early-warning works should be made available, so as to increase the level of societal awareness on this subject.

These efforts should also be matched with the necessary structures, procedures and mechanisms, financial and human resources as well as political will.

In order to do this, we must first acknowledge the fact that early-warning is a dynamic process of interaction between analysts

and policymakers. Therefore, efforts should be put into improving the communication channels between analysts and decision-makers.

The problem of cognitive biases of risk and threat perception can be partially overcome by relying more on computer models. Therefore, it is important to remember that, when warnings are based on beliefs, which contradict the recipient's *"established truths"*, their receptivity will decrease and vice versa.[34] To increase warning receptivity, regular interaction between analysts and decision-makers must be encouraged, as well as customizing warnings to different beneficiaries.

In addition, decision-makers should receive training on how cognitive biases operate in order to raise their awareness. Moreover, when communicated warnings should take into account cognitive biases, mainly *"loss aversion"* and *"psychic numbing"*. A possible solution should be to exploit lessons learned and good practices, while clearly emphasizing the costs of inaction[35].

References

1. Ciliers, Jackie, "Towards a Continental Early Warning System for Africa", *ISS Paper 102*, April 2005.

2. Comai, Allesandro, *Early Warning Systems For Your Competitive Landscape*, Society of Competitive Intelligence Professionals, vol. 10, no. 3, 2007;

3. Fusato, Massimo, *Preventive Diplomacy and International Violence Prevention*, October 2003.

4. Glantz, Michael H., *Usable Science 8: Early Warning Systems: Do's and Don'ts*, October 2003.

5. Hough, Michael, "Warning Intelligence and Early Warning With Specific Reference to the African Context", *Strategic Review for Southern Africa*, November 1st 2004.

6. Keyserlingk, Niels von and Kopfmüller, Simone, *Conflict Early Warning Systems. Lessons Learned From Establishing a Conflict Early Warning and Response Mechanism (CEWARN) in the Horn of Africa*, October 2006.

7. Kriendler, John, "Anticipating Crises", *NATO Review*, Winter 2002.

8. Lavoix, Helene, *Enabling Security for the 21st Century: Intelligence & Strategic Foresight and Warning*, 2 August 2010.

9. Matveeva, Anna, *Early Warning and Early Response: Conceptual and Empirical Dillemmas*, Issue Paper 1, September 2006.

10. Montaro, Lucia and Schünemann, Julia, *Walk the Talk: The EU Needs*

[34] Lucia Montaro and Julia Schünemann, *op. cit.*, accessed on 02.03.2012.
[35] *Ibidem*.

an Effective Early Warning System to Match Its Ambitions to Prevent Conflict and Promote Peace, February 2011.

11. Nyheim, David, *The Global Balance Sheet: Emerging Security Threats and Multilateral Response Capabilities*, The Stanley Foundation, October 2009.

12. Rogers, David and Tsirkunov, Vladimir, "Costs and Benefits of Early Warning Systems", *Global Assessment Report on Disaster Risk Reduction*, 2010.

13. Sawka, Kenneth, *The Intelligence Edge*, July.

Legislation

1. *National Defense Strategy* from 2010.

Internet Sources:

http://na.unep.net