The Institutionalization of Security Risk Assessment

Hari Bucur-Marcu *

When discussing the institutionalization of security risk assessment, the first reference that comes to mind is the NATO initiative that bears most directly on the subject, the Partnership Action Plan for Defense Institution Building (PAP-DIB).[1] In this document, the fourth objective calls for the development of "effective and transparent arrangements and procedures to assess security risks and national defense requirements." A reader of this objective would recognize that the phrase "arrangements and procedures" stands for the broader category of "institutions," and that the requirements for such institutions are effectiveness and transparency, for both the process of security risk assessment and the process of defining defense requirements. This article will discuss the significance of these requirements for the creation of institutions to assess security risks.

Effectiveness of Risk Assessment Institutions

Generally speaking, an institution is effective whenever it produces the outcomes that are expected of it. In order to translate this definition into the context of this discussion, I will identify two stages where the efficiency of defense institutions dealing with security risk assessment can be observed. The first stage is the regulatory process of providing appropriate arrangements, usually through national legislation, that properly define which national agencies are to be entrusted with the missions to identify, analyzes, and accept risks to national security. Such a definition process should also specify what documents these agencies shall publish, and with what frequency. These arrangements are supplemented by procedures established at the inter-agency and intra-agency levels, enabling them to actually perform the required security risk assessments. In fact, the institutional arrangements and procedures are effective if they are sufficiently accurate to guide these agencies through the process of security risk assessment (without being so minutely specific as to constrain the agencies' actions).

The second stage is the implementation process. The threats and risks to national security that are enumerated in the relevant documents are not just statements of legitimate concerns. They are also (or they should be seen as) powerful strategic arguments for the development of defense forces and capabilities that are able to defend national values, objectives, and interests against these threats and risks. In order for a response to be effective, the identified risks to national security should have a clear meaning for all interested parties. In terms of security relevance, the risk assessment should be meaningful for decision-makers within the defense establishment of a given

* Dr. Hari Bucur-Marcu is the Academic Coordinator of the NATO Studies Center in Bucharest, Romania.

1 Partnership Action Plan for Defense Institution Building (PAP-DIB), Brussels, 7 June 2004; available in the NATO Online Library, at www.nato.int/docu/basics.htm.

nation, for defense planners, and also for the international community. Moreover, in a democracy, it should be also meaningful for the nation's citizenry.

The PAP-DIB process was designed to offer particular relevance for the partner nations of the regions of Caucasus and Central Asia, as well as for Moldova. At the time when this initiative was introduced, in 2004, these nations had some legal provisions related to security risk assessment, but they published very few documents containing references to threats and risks to national security. And the relevance of these products to their security policies and defense requirements was somehow blurred.[2]

In the past, all these nations were very reluctant to express their security concerns based on effective institutionalized risk assessments. The existing legislation on security and defense was not very clear with respect to what arrangements were in place for justifying the preference for a certain size or type of military force, what capabilities it should possess, and what missions it should undertake. For a long period of time, these nations were merely considering which procedures they should enforce in their legislation or their governments' practices, with no visible results in the structure or capabilities of their military.

Only in recent years have they begun to contemplate incorporating the exercise of assessing the risks and threats to their security as part of their defense development process. They spent a great deal of time establishing what are the responsibilities of different governmental bodies for security risk assessment, or what are the steps they should follow in order to identify new force requirements. After these steps were completed, they begun deciding on preferred solutions and planning for force and capabilities development.

Even after these questions were answered by the relevant legislation, the actual process of identifying risks to national security was not yet as effective as it should be. One reason for this situation was that key strategic documents, such as security strategies or concepts, were very slow in appearing. And, once they were published, their implications for the development of defense requirements were still unclear.

One explanation for this arises from fact that most of the nations targeted by PAP-DIB did not have in place practices of issuing strategic political guidance on how security risks should be linked to defense missions and to military or non-military means and ends required for addressing those risks. Wherever the strategic security documents were published and were followed by relevant defense policy documents, one could observe some deviations from the provisions of higher-level documents in the lower-level ones. Not all the risks formulated at the level of security strategy were assumed at the levels of the defense or military establishments, or the defense documents

---

[2] In 2007, DCAF published reports on the status of building defense institutions in the nations of Caucasus, Central Asia, and Moldova, substantiating this observation. See Philipp Fluri and Hari Bucur-Marcu, *Partnership Action Plan for Defence Institution Building: Country Profiles and Needs Assessment for Armenia, Azerbaijan, Georgia and Moldova* (Geneva: DCAF, 2007); and Eden Cole and Philipp Fluri, *Defence and Security Sector Institution Building in the Post-Soviet Central Asian States* (Geneva: DCAF, 2007), both available online at www.dcaf.ch/publications.

introduced new risks that were not included in the original assessment.[3]

Under these circumstances, there was too much room for arbitrary or biased security risk assessment products, such as policies and strategies, or for rhetorical declarations about security concerns that were not founded on genuine assessments of security risks. The public interaction with the process of security risk assessment was sporadic and unpredictable.

Seen from the perspective of institutionalization, the effectiveness of the process of security risk assessment is less a matter of the actual content of the eventual risks that are identified and analyzed. It is more a matter of applying the principles of democracy to this process, especially the principles that the people are the supreme holders of power in a nation, and that the national security establishment exists exclusively to serve the people.

In this respect, the effectiveness of the institutionalized process of security risk assessment within a given government is revealed by the outcomes of the security risk assessment process. If the eventual risks that emerged from the process address the genuine concerns of the people, and the security threat implied by those risks bore directly on people's interests, aspirations, and well-being, then the process would be considered effective. Also from this perspective, the conclusion on the effectiveness of the process presumes that options open to the public are maximized, while the role played by the government's agenda is minimized.

This democratic exercise is relevant only if it leads to concrete measures that can be observed in the development of defense forces and capabilities. When security risk assessment is not followed by defense planning actions and does not engage national resources, the public will see the process as only political rhetoric and will soon lose interest in this issue, or will reject the government's actions.

Transparency of Security Risk Assessment

The public should be the key agent of validation of the effectiveness of security risk assessment, and transparency is a paramount condition for introducing the public into the equation. An important condition is that the public should be able to observe or even take part in the clarification process of risk identification and risk analysis, and be informed about political decisions regarding risk assessments. The most common transparency formats that serve as effective conduits of public interest into the process of security risk assessment are parliamentarian actions, such as testimonies and hearings; public debates organized and conducted by governmental and nongovernmental organizations; and the possibility for members of the public to express alternative opinions in publications available to a wide audience.

In any democracy, risk assessment is a very delicate task for the government. On one hand, the public forms its own perceptions on security threats and opportunities, which forces the government to factor public opinion into its political decisions. Thus,

[3] Fluri and Bucur-Marcu, *Partnership Action Plan for Defence Institution Building: Country Profiles and Needs Assessment,* 27.

these decisions would reflect not only government opinions but also popular ones. For the nations formerly belonging to the communist system, this would represent a huge leap forward. In communist times, it was assumed that the government (or the leadership of the Communist Party) always knew best what were the interests of the people, and the people were never to question the trustworthiness of Party political decisions on security affairs.

In the new political system, however, the involvement of the public in the process of security risk assessment actually imposes more order in this area of government activity. The process of risk assessment involves interagency actions, where each agency brings its own agenda to the discussion. Moreover, the government has its own political agenda that sometimes biases the process of identifying security risks. Without comprehensive democratic oversight, some risks that are irrelevant to the public interest but that threaten these political agendas might find their way onto the list of risks to national security, and eventually divert resources and energies from genuine national security concerns.

Transparency is also important because risk assessment is part of the process of assessing the security environment, along with the assessment of security opportunities and challenges. It also proceeds hand-in-hand with the development of strategic visions and the identification of national values, goals, and interests that should be defended and/or promoted with military means. All these topics are subjects of public debate and popular acceptance; hence transparency is a must if these decisions are to achieve a broad base of consent.

The Strategic Value of Transparency

There is another incentive for rendering this process and its outcome transparent, an incentive that derives from the strategic value of the risk assessment itself. Risks and threats revealed and explained in national strategic documents, such as security concepts or strategies, are the key ingredients of the permanent dialogue among governments in the international arena, and between each government and its people on strategic security issues. Unless a nation has a predilection for aggressive military actions, the main rationale for any nation to develop any sort of military power is to defend herself from whatever threats and risks exist that pose a challenge to her objectives, values, and interests. This situation highlights the important place risk assessment occupies at the strategic level, both domestically and internationally.

Risk assessment is so important in strategic terms that even the domain of national and collective military power is nowadays referred to as "defense," meaning that it is reactive to threats and risks. In this context, it is not only the risks and threats with strategic value—usually those risks that challenge the very existence of the nation, the freedom of her people, her independence, integrity, and sovereignty, such as military aggression—that have strategic importance, but all risks and threats that justify the development of military forces and capabilities.

It is important to note here that the international community is sensitive to the transparency of risk assessment in any given nation. For example, the nations for which the PAP-DIB process is particularly important are members of the Organization for

Security and Cooperation in Europe (OSCE), and all recognize the OSCE Code of Conduct on Political-Military Affairs and the OSCE Defense Planning document. Both these security enhancement instruments contain clear provisions that are in line with the requirements of democracy and justification of defense forces based on requirements derived from transparent security risk assessment processes. Of course, these OSCE initiatives are only politically binding, and the states are free to implement them at their own pace. But they clearly indicate that these requirements are key ingredients for enhancing peace, stability, and confidence building among the member states of this organization.

Three Levels of Transparency

The main question is what "transparency" exactly means in practical terms. The answer can be found at three levels: institutions, policies, and risks. At the *institutional* level, this means that the arrangements and procedures that are stated in appropriate legislation and regulations and that address the process of security risk assessment should be transparent. They should explicitly determine which governmental bodies are entrusted with the responsibility of identifying and analyzing security risks, and which are empowered to make political decisions based on the work of the former. These arrangements and procedures should also establish the periodicity of the process, as well as the formats of documents in which the assessment is presented to the government and the public. All these aspects are important to building public trust, as they give the interested members of the public relevant information on how the government is organized to act on their behalf in this specific field of security risk assessment.

The *policy level* addresses those policy documents where the security risk assessment is published. The term *policy* has different meanings, according to the context in which it is used. In our case, we are looking for those documents issued at the security sector level (i.e., national security strategy/concept, strategic vision), and at the defense sector level (i.e., national defense strategy/white paper/strategic defense review). For the purposes of translating the assessed security risks into defense requirements, it is also important to consider military strategy, where the relevant risks identified at the security sector level are incorporated and reassessed from a military perspective. All these documents should be part of the public record – that is, the public should have unrestricted access to them. More and more nations are extending the transparency of these policies and strategies to the elaboration process, publishing drafts and inviting the public to express opinions on those draft documents, under the requirements of a transparent public administration decision-making process.

The level of *risk* describes the actual content of comprehensive statements addressing categories or clusters of risks, grouped according to criteria such as the relevance of those risks for national security (i.e., challenges to national values, goals, interests, territory, economy, public safety, etc.); their nature (i.e., military/non-military, natural/industrial disasters), and their urgency (i.e., immediate alarm, or longer-term warning). These statements should also identify those security sector organizations that have main responsibility for each form of threat, and should specify the distribution of supporting roles for each type or category of risk (i.e., defense forces taking the lead,

with civil emergency forces in a supporting role). This process of role identification will lead to the development of strategic missions for the respective security and defense forces responsible for addressing those risks and threats.

Challenges to Security Risk Assessment

The integration of the process of security risk assessment into the processes of defense policy formulation and implementation by no means follows a linear path. There are several challenges a government has to overcome in order to make this process effective and transparent.

One challenge is that security risk assessment never represents a fresh start in the development of defense forces. At any moment in time, when a new risk assessment is published, there is already a defense system in place, based on requirements derived from risk assessments performed years ago. Some of these security threats and risks might still be valid, some might be obsolete, and might no longer be possible to mitigate through existing military means.

Assuming that the process of connecting identified security risks to the development of defense requirements is fully institutionalized, the re-evaluation of already existing threats and risks would result in re-evaluation and eventually re-configuration of the defense structures, forces, and capabilities. This situation would add new levels of complication to the effort to build new defense requirements resulting from the introduction of new threats and risks. It always requires significant determination for the politicians in power to voluntarily revise already identified risks and to assess new ones, when they know from the beginning that this exercise would result in supplementary efforts and costs.

Another challenge results from the inherent political sensitivity of some of the risks, especially when new risks are not fully explained to and understood by the public. The government would prefer to address such risks behind closed doors instead of doing so in a public forum. But, at the same time, the government is obliged by the strategic importance of risk assessment to ensure the full transparency of this process. It is easy to say that, when facing such a secrecy/transparency dilemma, a democratic government should always decide the matter in the favor of transparency. But in real life, governments always have to find the right balance between the two, and that is in itself a challenge.

We may also identify a challenge at the very level of institutionalization. The challenge is for legislators to clearly delimitate responsibilities and tasks to different governmental agencies involved in security risk assessment. Each nation has its own approach in institutionalizing the process of security risk assessment. Generally speaking, the main components or stages of this process are risk identification; risk evaluation; risk prioritization; and risk acceptance. The legal and organizational arrangements and procedures in place assign one or more agencies to each of these stages. They should enhance effectiveness and transparency, but they also should pave the way to a collaborative approach to security risk assessment.

The risks and threats emerging from this process gain in importance in relation to the consequences they imply for the security and defense establishments. Defense pol-

icy documents stating the perceived risks to national security should also establish a visible correspondence between the assessed risks and national defense requirements; otherwise, statements of these requirements will appear to remain purely in the realm of rhetoric. There are risks that allow for a political or practical decision to be made as to whether the risk should be addressed by military or non-military means, just as there are risks that can be addressed exclusively by military means, or risks that should have no military implications.

In an institutionalized process, the agency or agencies entrusted with the task of identifying threats and risks to national security should restrain itself or themselves from pre-judging the implications of the risks that are identified for defense requirements. Ultimately, it is up to the political establishment to decide what risks should be countered by military force, and what should be addressed by non-military means, or not be addressed at all.

Risk identification is usually the responsibility of intelligence agencies. These agencies also perform analyses and forecasts of the internal and external security environment. Due to their specialized nature, they tend to be perceived as an authoritative voice on every aspect related to risk assessment, even those that are well beyond the natural scope of their responsibility.

Risk evaluation is the stage where the identified risks and threats are measured in terms of their relevance, importance, or urgency to national security. It is obvious that this stage can no longer be solely under the control of intelligence agencies. It requires more inter-agency cooperation, with each agency bringing in specialized knowledge and expertise in various fields of national security.

Risk prioritization addresses the question of preference among multiple alternatives. This is already a political decision, and should be performed by political bodies of the security and defense sectors.

Risk acceptance, namely the endorsement of the risks and threats that have been identified in the assessment process, and then evaluated and prioritized by various governmental agencies and compiled in a strategic document, is not only a political matter. It is also a matter of democratic representation. This stage is also the ultimate expression of democratic control and democratic oversight of security and defense, and is usually performed by legislative bodies.

Conclusion

Looking at the way the Partner nations from the regions of South Caucasus, Central Asia, as well as the Republic of Moldova are approaching the PAP-DIB objectives, we may agree that the process of security risk assessment is gaining momentum in most of these nations. Perhaps more importantly, we can look forward to the time in the not-so-distant future when this mechanism will replace the more opaque and arbitrary procedures that are currently used to determine defense requirements in these countries. The experiences of these nations can help serve as a model for other states that are working to implement the PAP-DIB objectives and achieve the required levels of transparency and effectiveness in how they assess security risks.

Bibliography

Cole, Eden, and Philipp Fluri. *Defence and Security Sector Institution Building in the Post-Soviet Central Asian States* . Geneva: DCAF, 2007.

Fluri, Philipp, and Hari Bucur-Marcu. *Partnership Action Plan for Defence Institution Building: Country Profiles and Needs Assessment for Armenia, Azerbaijan, Georgia and Moldova* . Geneva: DCAF, 2007.