INTERNATIONAL CONFERENCE RCIC'17
Redefining Community in Intercultural Context
Bari, 5-6 June 2017

THE 3D [TRIDIMENSIONAL] ORGANIZATIONAL SECURITY STRATEGY MODEL

Bogdan N. ȚUGUI

Mihai Viteazul" National Intelligence Academy, Bucharest, Romania

Abstract: *Within the current global environment the strategy is a prerequisite concept for the development of any organizational security policies. The added value of a brand distinctive strategic security concept is vital for protecting the assets of an organization. Hereby, an innovative security strategy model is corroborated and proposed with a view scrutinizing the requirements for a"3D [tridimensional] Organizational Security Strategy". This model presents the strategic vision resulted from the paradigm shift into the fields of security; identifies certain dilemmas and discrepancies identified into the current environment of the existing security policies; and discusses the impact of a security strategy. This approach is based on a 3D [tridimensional] strategic vision that brings together: (1) the traditional approach based on urgency (hard security), (2) the client oriented approach (soft security), and (3) a structured policy vision (structured security). These tree elements together are today`s driving factors within the organizational security environment. Further on, all supporting policy documents into the field of security shall follow the path of the policy line endorsed by the security management of an organization. These issues require further analyses, assessments, amendments and endorsements*

Keywords*: strategic security concept; 3D organizational security strategy; hard security; soft security; structured security*

1. INTRODUCTION

1.1 **Vision statement.** Security has undergone a paradigm shift. The traditional notion of security has evolved throughout the last decades into some new global conceptions (i.e. societal security, human security, common security, comprehensive security, hard & soft security). The consequences now of the paradigm shift are the new parameters set generally and globally for security policies. The organisations shall acknowledge the paradigm shift for elaborating viable security policies. This document suggests that the shift is necessary, from one linear security dimension based on the urgency of events, towards the acknowledgment of a tridimensional [3D] security strategy based on: (1) urgency, (2) client oriented approach, and (3) structured policy vision.

1.2 Purpose. The purpose of the 3D Strategy is to provide a framework for the development and review of security policies within organisations, the identification of operational requirements and the setup of a professional development agenda into the field of security within an organisation.

1.3 Scope. The scope of a 3D strategic vision is to achieve, support and enhance the overall goal lines of an organsiation through communication and partnerships with all relevant stakeholders.

1.4 Definitions. For the purpose of this document, the following definitions (ASIS International, 2017) shall apply:

"Assets" means anything that has a tangible or intangible value to an organisation; assets are tangible (e.g. personnel, facilities, documents, materials) and intangible (e.g. reputation, information, human health and safety in every aspect related to work).

"Client" means organisation or person that receives a product or service.

"Organisation" means group of people and facilities with an arrangement of responsibilities, authorities and relationships.

"Security" means the condition of being protected against hazards, threats, vulnerabilities, risks, or loss.

"Policy" means overall intentions and directions of an organisation as formally expressed by top management.

"Strategy" means a plan or a method designed to achieve the major or overall aim of a policy.

2. BACKGROUND

The new security paradigm has merged concepts like societal security, human security, common security, comprehensive security, hard & soft security, and has set the norm of the present-day security policies within organizations as well.

The organisations have adopted brand distinctive security concepts reflecting for example their public/governmental or private/corporate strategies. The governmental or the corporate security models respectively represent the institutionalized design of the public, or private facets, in the respective fields of security. It is often the norm that the corporate security strategy line becomes more inclusive and replaces, with time, the extractive line set previously by security governmental models within the remits and the facilities of an organization. More often that rare, security activities within organizations have been driven mainly by urgency and were based on the rhetoric of events, while the strategy & the vision a security policy have remained continuously under development. The rhetoric in such cases cancan become more promising than the policy can actually deliver. The rhetoric referred into such cases to advocating, only vocally, the necessity for balance and normalization of the organizational security requirements through the lenses of the respective organization clients and stakeholders.

Organisations have adopted brand distinctive security concepts. The institutionalized design of security set by the governmental organization has often imported norms set first within the lines of the corporate security strategy. The corporate style has been proactively adapting to its global endeavors. This adaptation is thought to match the parameters and the interest of the inclusive organisations. The settings of the inclusive organisations encourage participation by featuring a system of law and provision of service that provide a level playing field for its stakeholders. It is the nowadays norm that the security discourse refers to treating a specific incident matter in a structured way, managing incidents as a process, exercising and reviewing management processes in the field of security, establishing reporting processes for security incidents and emergencies, etc. The role envisaged, for the modern approach of structuring the processes in the security field, is to transform inputs in outputs and implement lessons learned with a view towards establishing an early warning system for organisations.

The structured approach implies also that scientific formulas, graphics and technical workflows, for example represent currently a solid frame for the sound judgments provided to the management levels of an organization. Thus, one would say that the linear dimension of hard security set previously by the urgent need of imposing or keeping afloat an organisational security standard, has turned now close to the field of science or even being a science in itself.

But can security be considered also an art? The security professionals are often prompted with notions or requirements implying that accent should be focused as well on selling security, being client oriented, and searching soft security alternatives. It turns first as an imaginative art and only then as practical alternative for a hard security liner to accept the benefits of this alternative. That is because, instinctively, the alternative looks relatively as a palliative care rather than a straightforward treatment medicine. So where do we make the compromise? This is something that the parts involved must work on together, to set the policies to what *enough security* shall be, and how enough design and process elements shall be implemented.

A new dimension is empowering nowadays the concepts of security strategy, influenced by the advocates of soft security ideals. It is often the case that at present the expression "client oriented" has seized the floor of the security industry. Thus, organizational security has come to the point of being rather "sold" to its clients and beneficiaries, in order to be accepted internally to its ends. The real challenge comes from where rhetoric ends, as it happens also when the polls have closed following electoral campaigns, when the volatility of political discourse, as an act of speech shall be transposed into practice by changing the party settings, from the campaigning lobby, back to governance mode.

The strategy illustrates the plan and the method designed to achieve the major or overall aim of a policy. The security strategy of an organisation shall refer to the plan or the methods designed to achieve the major aim of the overall policies throughout the organisation – and not just the security policy in itself. The leadership of an organisation defines the strategy. An important characteristic of leadership direction and support is promoting excellence in policy development. One of the best ways to communicate this is through the understanding of the policy development processes, which include: establishing the actual need for regulating via policies, development of a policy team, policy implementation and the policy

execution phases. It is essential for the leadership to ensure and check if the scope of an envisaged policy is cross-functional throughout the organisation or it is simply designed to impact the security operations. The daily issues of an organization have multiple facets and layers, involving more than one departmental unit and stakeholders. Thus, the strategy of a successful policy development is to identify and involve the clients and the stakeholders in this fledging process. By identifying, accepting and involving from the beginning the key stakeholders in this process, the policies will be keenly accepted and more effective.

Security is an ever changing field where new threats are arriving and new concept design elements are constantly becoming available as well. The real challenge is surpassed and a real sense of assurance is achieved only when the "mocking plan" is implemented, for bridging the hard line of reality with the abstract parameters set both by security as a "science" and as an "art".

Therefore, in order to transpose the shift and the security paradigm into practice, robust security policies should be implemented within organisations. The challenge is present already and the paradigm shift has happened. Thus, is necessary to acknowledge that the shift is necessary also for the security practice, from one linear security dimension based on the urgency of events, towards a tridimensional [3D] security strategy that takes into account: (1) the *urgency,* (2) *the client oriented approach,* and (3) *the structured policy vision – managed as a process*.

3. THE 3D SECURITY STRATEGY

3.1 Urgency (hard security). Urgency is often set inadvertently within organizations as the main dimension of their security policy. Admittedly, urgency is pervasive and cannot be eliminated; it represents a domestic approach that provides legitimacy for the security sector; it is also the dimension where hard security operates – as a concept applied for the direct confrontation/ approach of an event. This doesn`t mean that the security of the organisation is underdeveloped. It rather means that it served for the practical purpose of crisis/emergency – response within an organisation.

3.2 Client Oriented (soft security). The client oriented dimension empowers the concept of soft security as an induced feedback to all administrative apparatus of an organisation – hence, also the security apparatus. Note: Client oriented approach means a group of actions taken to support operational activities and services in considering client needs as major priorities. That group of actions includes: developing a quality product appreciated by the clients; responding promptly and respectfully to queries and complaints; dealing sensitively with organizational issues.

The clients (stakeholders) of security can be mainly identified within the personnel working within the organisation (i.e. staff members, interns, interims, contractors, visitors). Thus, the personnel of an organisation have been considered one of the prime referent objects for security activities. However, in a broad sense the notion of stakeholders includes also: local/governmental agencies (i.e. local police, fire brigade, gendarmerie), other various agencies & institutions, some NGOs, or even third countries linked to an organisation. All these stakeholders are today players into the field of organizational security.

Their interaction has caused a "normalization" of security. It means that security is not anymore resulted from the interests of a sole party; security is now negotiated and leveled to the particular needs and expectations of all the stakeholders. As a result, security has turned sometimes into an act of speech and has been even included on the "political" agenda. It means that stakeholders often refer verbally to a specific event as critical – hence the urgency for security to intervene. The "political" aspect refers to security as influenced by the partisan interest of its stakeholders – as end users/clients/beneficiaries - who can influence, decide and attune the security activities of an organization.

3.3 Structured policy vision (structured security). The structured security approach was introduced with a role to facilitate the decision making process, which should be based on sound analysis supported by the best data available. Organisational security measures shall be determined based on a Risk Management Process. This approach has introduced a *structured* method for the security activities and to create the prerequisites for a *security early warning* system at Eurojust.

The concept of the Risk Management Process is aiming towards transforming the operational inputs into security outputs. This model is currently foreseen for implementation into the security rules of the international organisations and institutions[1], with respect to the security measures

[1] see for example: Council Decision on the security rules for protecting EU classified information (2011/292/EU); Decision of the Bureau of the European Parliament concerning the rules governing the treatment of

to be determined for protecting personal data, and sensitive or classified information. What if there is no such sensitive data or classified information, acknowledged as such, within the premises of an organization, consequently requiring a protection level scrutinized under the security rules? Most of the organisations do not handle for example classified information throughout their activities process. Furthermore, it is a comfortable temptation for the high leadership and management levels directing the lines of the organisational security policy to falsely acknowledge that the sensitivity level of the information or the personal data handled by the organization do not impose or need to elaborate further any security rules in that specific case. However, one should not forget that security shall be directed towards protecting the organisational assets, whereas "assets" means anything that has a tangible or intangible value to an organisation; assets are tangible (e.g. personnel, facilities, documents, materials) and intangible (e.g. reputation, information, human health and safety in every aspect related to work). Consequently, the fact that something (or someone), if not labelled as classified, can leak to public at no costs it is a bias that shall be avoided. Certain assets, enumerated above in their generality, are not considered under a "classified" regime. However, public knowledge of alleged negative organizational characteristics concerning for example the reputation (which is one of the assets) of an organization can impact adversely, if not in a disastrous capacity, the grounds of the very existence of an enterprise. It is therefore necessary for organisations to develop security policies with a view to protecting the integrity of their tangible and intangible assets.

The concept of the Risk Management Process transforming inputs in outputs has also an essential role for establishing an early warning system within organisations. Such a system shall be an operational tool for the security of an organisation, providing information on identified risks, forecasting and giving sufficient time to prepare resources and response actions to minimize a negative impact over the assets of the organization.

3.4 The policy impact of the "3D" Security Strategy. The security policy is an extremely important tool in the intra and inter-organisational context. The added value of the "3D" strategic vision is that it does not identify the matter as a "lack of something" or as a "need for something" but structures the incidence of impacts – the interactivity of its dimensions – as a policy problem illustrated with qualitative and quantitative indicators. The model identifies the defining elements of security, as they exist naturally within organisations, and presents them emerged in a format that illustrates the way forward. The "3D" strategy is rather about seeing and acknowledging the security architecture of the organisations projected strategically into a pragmatic future.

The "3D" strategy model indicates the structured method to engage and maintain contact with all affected stakeholders, using the appropriate tools and format to reach them. More importantly, the "3D" strategic vision can offer the option to distinguish the viable synergies and confirmatory feed-back that can be extracted from the opinions of stakeholders. The strategy line determines the policy and its viability. The adoption of a viable security policy developed on the platform of a "3D" strategy will tackle the discrepancies emerged from any convergent interests within the organisation. Security policies cannot be implemented within an organisational vacuum. Just as the support of the senior leadership cannot be overlooked, so does the input of the stakeholders. A successful security policy requires the use and consideration of every functional area within the organisation, including Human Resources, Legal Services, Information & Technology, Budget & Finance, Public Relations, Facilities & Logistics Management, Administration Unit, etc. After all, the term security refers the condition of protecting the assets against hazards, threats, vulnerabilities, risks, or loss. The assets of an organisation can be identified in any of the above mentioned departments, whereas the term assets refers to anything that has a tangible or intangible value to an organisation; assets are tangible (e.g. personnel, facilities, documents, materials) and intangible (e.g. reputation, information, human health and safety in every aspect related to work).

Communication and intercultural aspects may constitute an important obstacle prompted against the dimensions of the "3D" security strategy. First, as it is often the difference between "saying it" and "doing it", it is often the case that a formal security policy proposal does not match the expectation of one stakeholder and is therefore contested – although the policy goes through and is formally adopted by an organisation. The solution can only be to structure the communication and identify the

confidential information by the European Parliament (2011/C 190/02); Decision of the High representative of the Union for foreign affairs and security policy on the security rules for the European External action Service (2013/C 190/01).

common grounds for discussion. It might be often the case that the standoff is due to another formal policy, existing already, which upholds a segregated interest of a stakeholder, and shall be reviewed under the ”3D” lenses as well. The policy is not just a document or a piece of paper, but rather a security tool that shall be designed to be viable and feasible. It is the constant determination, applied within a process of organisational balance and checks, which indicate eventually the silver lining of a policy agreement.

The risks associated with a poor consultation process of the clients and stakeholders can otherwise determine: limited understanding of the problems; poor policy solutions; lack of policy coordination; negative clients' reaction to a policy. When defining the parameters for the security policy, certain industry standards can oppose different meanings to common definitions used inadvertently, although with opposed meanings to different stakeholders. For example, while it is of a tantamount importance to define, within a security policy, terms such as “security investigation”, which might be of a general significance for all fields of security at the EU institutions and organisations, it appears that the bar was already set high and the definition was allocated only to personnel security clearance requirements:

> ’Security investigation’ means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a national or EU PSC [EU Personal Security Clearance] for access to EUCI [European Union’s Classified Information] up to a specified level (…) (2011/292/EU).

Analysing further on the divergent implication of the definition: the management level approving such a security investigation pertains only to the competent authorities of the EU Member States and the management level approving it is located within the head quarters of their National security Authority, whereas the “local” organisational endeavour would be rather to define and determine within its premises the grounds and authority approving the “security investigations”.

Should one make an attempt to conciliate the definition in this instance (security investigation) to its mundane usage, the solution at hand is rather to acknowledge that the standard was set already by the higher policy rules, and the solution would be to coin another particular term for the specific investigation context: for example “physical security investigation” if one would like to refer only, in a security policy, to the field of physical security in an explicit manner.

3.5 Boundaries and synergies. The security apparatus of an organisation is acting often as a gateway for all the various matters while its own specific security tasks are also increasing. Therefore, the boundaries of the internal security architecture must be clearly defined and delineated within an organisation. A viable security policy shall establish a clear framework for exploiting and capitalizing all the synergies (with regards for example to activities into security related fields such as physical security, safety, security of information and communication technologies systems – ICT security, classified information security and personnel vetting, etc).

Security related activities may find a common playground where operational interests interact individually. The effect of the interactions should be capacitated towards producing synergies rather than a frustrating duplication of efforts. The effect of such synergies can be rather transposed under the umbrella of the “3D” strategic platform which can be used for structuring the security activities into a more competitive manner, considering the pallet and the synergies projected from each of its dimension into a field of interest of the organisations. For example, for the attempt made to identify a structure for the various specific security tasks assigned in an organisation, we can use the notions of *specialities* and of *specialisms*. This conceptual approach for structuring security activities implies that a

> “specialty” is a class that includes more than one “specialism” – the last being a concentration of one's efforts in a narrowed occupation or field of study; it illustrates the specialty as a “bubble” of main security tasks; and the specialisms skills that are included into such a “bubble”.

Thus, certain security tasks should be grouped under a speciality which requires furthermore the specialism of certain skills in security. A structured model of security *specialities (i.e. specialisms)* is suggested below:

[1] *Facilities Security* (i.e. security of organisational premises, safety & fire prevention, scheduling, supervising and monitoring the security performance of personnel, security training assurance, emergency response, etc);

[2] Executive Security (i.e. VIP`s escort & executive driving, security of meetings & conferences, security measures for external activities and missions, etc);

[3] Technical Security (i.e. keys management system; pass & ID, safes management, card readers, access control, CCTV systems, X-ray security screening, X-ray safety expertise, Technical Surveillance Countermeasures - TSCM, secured radio communications, maintenance of security technical equipment and installations, etc);

[4] Process Management Security (i.e. risk assessments, business continuity planning, security awareness presentations, investigation management, open sources intelligence/security cooperation & liaison, development of security policies, development and implementation of early warning capabilities, etc);

[5] ICT security (i.e. testing, implementing plans, products, controls, related to the security of the information and communication technology);

[6] Information security (i.e. data protection, security clearance, registry, classified document management);

[7] Intelligence (i.e intelligence, counter-intelligence, counter-intelligence, OSINT, etc).

The concept of a "3D" security strategy provides a better framework for reviewing and developing of the organisational security policies, the identification of operational requirements and the setup of a professional development agenda into the field of security within an organisation. That is because the process of corroborating the synergies of its three dimensions determines a more accurate map of the incidental issues and challenges perceived now from a "3D" perspective.

The definition and parameters of what is actually a security incident shall be defined, based on each organisation's profile, and then transposed formally into the internal policy documents. Inadvertently, statistics kept by organisation would indicate the numbers of the certain security incidents registered each year. Differences concerning the extent to which a certain fact occurrence would constitute or not an incident, from one organisation to another, should be determined not on ad-hoc organisational reaction determined by the urgency of events, but rather on the identified parameters and based on risk assessments which can pre-determine for example the organisational risk appetite, the preventive measures or the mitigation factors taken in response to the vulnerabilities underlined by a specific incident.

4. CONCLUSIONS & ACKNOWLEDGMENT

4.1 Conclusions. The 3D Strategy has yet generated more questions than answers. Arguably, throughout debates, some opinions have questioned: the utility of a Strategy – just as another paper that doesn't say much; the client-oriented approach - as a utopic dimension of the traditional security feature; the structured security dimension (synergies' identification, specialty/specialisms structure) – as a pretentious transposition of the basic security related activities. Nevertheless, opinions stated that such a strategic vision – if needed after all – should be drawn at the highest security management level of an organisation. Security has evaded from its traditional boundaries. A strategic approach is vital for protecting the assets of an organisation. This paper presented the strategic vision resulted from the paradigm shift into the fields of security and has advocated that a "3D" strategic approach represents a feasible and practical security solution. The "3D" Strategy model shall be referred for further analysis, assessment, necessary amendments and managerial endorsements – as applicable. The security policy, like other (generic) policy documents shall follow the path of the policy line endorsed by an organization.

4.2. Acknoledgement. The author takse full responsibility for the contents and scientific correctness of the paper.

BIBLIOGRAPHY

1. ASIS International. (2017). *ASIS Online* [online]. URL: https://www.asisonline.org/Pages/default.aspx. [Accessed on May, 2017].
2. Buzan, B. [1991], (2009). *People, states & fear an agenda for international security studies in the post-cold era.* Colchester: ECPR.
3. Kirchner, E. & Sperling, J. (2007). *EU security goverance.* Manchester: Manchester Univ. Press.
4. David, D. (2012). *The beginning of infinity, explanations that transform the world*. London: Penguin Books.
5. The Council of the European Union. (2011). Council Decision of March 2011 on the security rules for protecting EU classified information (2011/292/EU). *Official Journal of the European Union.* I. 141/17. May 27.