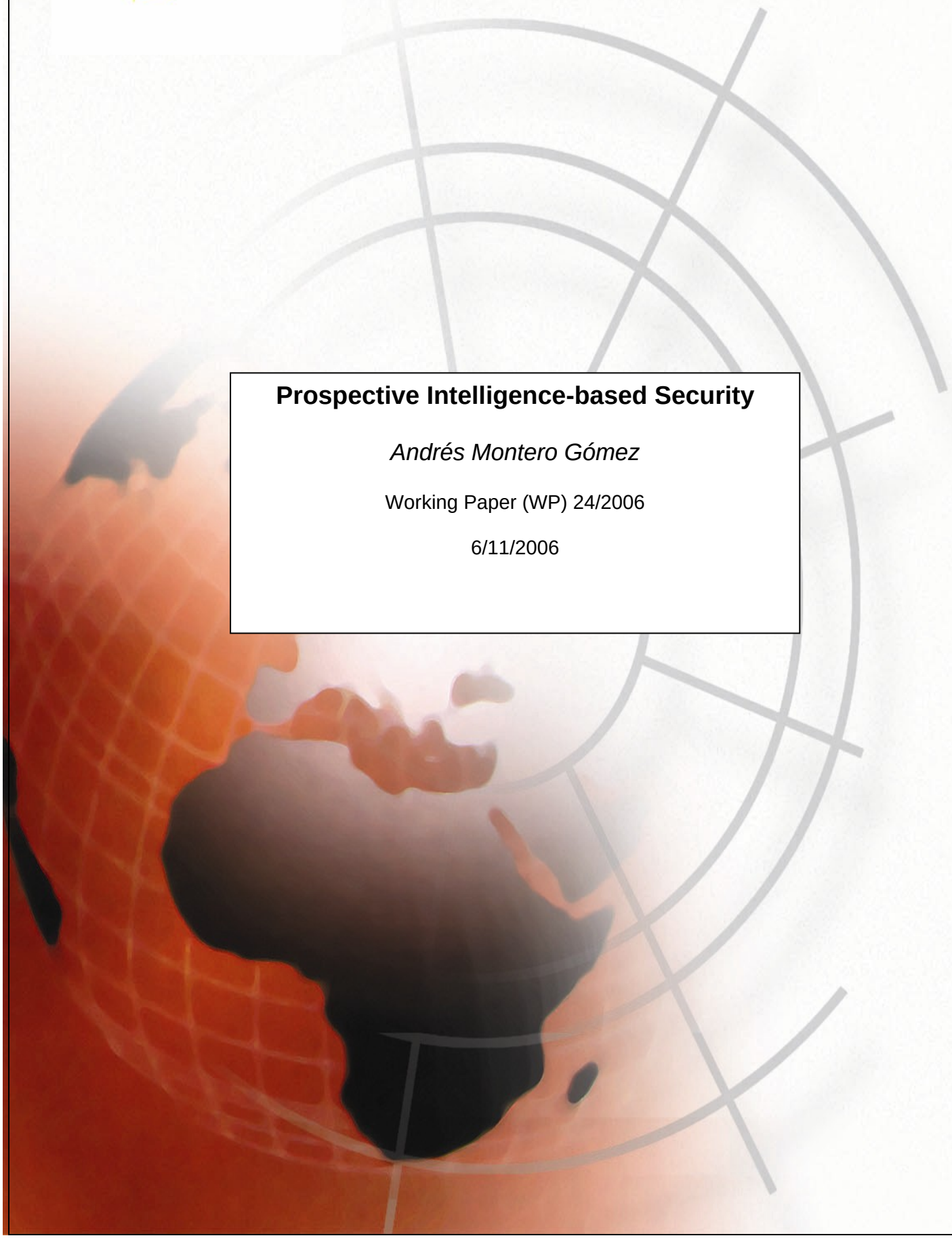

Prospective Intelligence-based Security

Andrés Montero Gómez

Working Paper (WP) 24/2006

6/11/2006

Prospective Intelligence-based Security

Andrés Montero Gómez [*]

Summary: Jihadist terrorism and global organised crime have not only challenged traditional concepts of domestic and foreign security, but are making evident that reactive security or security that is separate from intelligence are obsolete responses by States to threats.

Introduction[1]

Jihadist terrorism and global organised crime have not only challenged traditional concepts of domestic and foreign security, but are making evident that reactive security or security that is separate from intelligence are obsolete responses by States to threats. The development of prospective intelligence-based security doctrine, methods and bodies is presented here as a structural option to provide security institutions with capabilities for intelligent, preventive and pro-active responses to emerging threats.

Public security is a concept that cannot be reduced to a response based solely on policing, but should be a 'horizontal pillar' of citizens' freedom which should confront all the elements that contribute to generating vulnerabilities in the face of threats, in unleashing them and in maintaining them in the social fabric. To offer a functional, efficient and effective response the authorities must adopt intelligent security approaches based on the comprehensive knowledge of the threats. This knowledge should be based on a thorough descriptive analysis of the phenomena, and on the subsequent explanation of their causes. Knowledge-based intelligence is the basis from which security institutions will be able to undertake prospective studies to support decision-making in the application of preventive security, reducing the risks by managing the uncertainties.

Response: From Reaction to Prevention

Within the continuum which security sciences might represent, "hard" approaches of security are a far cry from the flexibility, ambiguity, globality and versatility of current social threats. These threats, which are cross-border phenomena, no longer even respond to the traditional configuration of an element which seeks to cause damage in order to obtain benefits. The leitmotiv of terrorism and organised crime is to take advantage of the system's weaknesses in order to benefit illegally. Similarly, they assume that in order to obtain these benefits they must exercise violence and impose force. Causing damage is factored into the equation and, in a way, particularly in terrorism, is instrumental. In contrast, other threats which are currently affecting our societies, such as immigration or those deriving from environmental imbalances do not entail that component of deliberately inflicting damage but rather emanate directly from dysfunctionalities inherent to the very social system which we have built and, from within it, threaten its well-being, its stability and, therefore, its security. Modern security thus understood should therefore transcend the traditional concept of a response to an aversive threat administered intentionally by

[*] *Coordinator of the Prospint Programme of the Office of Spain's Secretary of State for Security*

[1] The opinions expressed in this Working Paper do not represent any organisation or institution.

external agents, to become a configuration of schema, situations or structural dispositions which not only respond but actually anticipate and foresee risks which potentially erode or undermine the chosen or established modes of co-existence.

The governance of our security is still too biased towards executive reactive response measures, with scant input in terms of structural anticipation taking into account the multi-dimensionality of democratic remits vis-à-vis the complexity of new threats and, naturally, too oriented towards tough security measures, whether political or defensive. Our security systems do not envisage the global disposition of risks. Nor indeed do they consider the need to take into account social involvement and participation, above and beyond public institutions specialising in reactive security, in dealing with them. Having said that, in regard to threats which introduce intentional social damage into their horizon of benefits, such as terrorism or global organised crime, not even security systems have managed to adapt their focus to the nature of the challenges. For decades, the treatment of security threats has consisted in a symptomatic approach, not based on etiological knowledge of the phenomena, but on offsetting their presence and their harmful effects. The result is that threats, such as drug trafficking or terrorism, are contained at structural levels, remaining as chronic social ills, whose deep-rootedness is sometimes further strengthened by the response policies themselves.

In a society of knowledge, intervention based on knowledge, and therefore on evidence, is increasingly seen as an effective measure in articulating response schemas; indeed this is forcibly so if the aim is to afford them any anticipatory or preventive properties. Knowledge-based security is intelligent security, based on processes of compilation, evaluation, analysis and interpretation of the information on threats which unlock the codes of a behaviour which might be forecast with acceptable margins of error.

Intelligent Knowledge-based Security

The adequate development and implementation of intelligence skills, procedures and measures are currently considered to be key factors in successfully combating organised crime and global terrorism in the long term.[2] In the so-called security sciences, intelligence encompasses activities, processes and institutions devoted to obtaining, processing and disseminating information in regard to areas or objectives that are of interest to a nation's security.

The new threats are not new. It is true that we sometimes refer to them as new in order to somehow mentally justify our delayed response to them... if they are new, we tell ourselves and others, we will need a little time to get to know them and to dismantle them. In fact, they are the same threats as always, but evolved, in a wholly Darwinist sense, to adapt to –or perhaps to help determine– the nature of global society. Furthermore, public security has also evolved: internal structures of security institutions have been modernised; those responsible for security have adapted their management styles to include the most widespread management techniques; security professionals join institutions with acceptable levels of formal education; we have been quick to embrace new technology... yet public security institutions are still slow and cumbersome, highly bureaucratised, and they are highly conservative and trapped by their own significant aversion to risk. Quite the opposite is true of the threats which they are up against.

Global threats, which can be labelled collectively as global organised crime, have some very distinctive features: they are international, they are horizontal in structure, and they are diffuse, interconnected and intelligent. To continue with the Darwin simile, in reference to organised crime or terrorism, intelligence of crime is understood as the capacity of

[2] A. Montero, 'Crítica de la razón bélica contraterrorista', *Revista Sistema*, nr 193, July 2006, p. 121-129.

criminal groups and networks to adapt to a hostile environment, monitored and scrutinised by permanent security devices, in order to achieve purposes which infringe the established limits of rules of conduct, which in this case are based on compliance with the law. The progressive changes in the Latin American cocaine cartels or the increasing sophistication of money laundering methods by organised crime rackets are examples of adaptability and intelligent behaviour; piloting commercial aircraft on domestic routes in the US to use them as huge explosive devices aimed against important symbols of our civilisation, conveying a multilevel message to a range of audiences by means of devastating criminal acts, is another tragic example of lateral thinking which adapts to the predictability of our planning. Of course this intelligence we referred to is not related to any moral use of the term, but even if we were to debate this issue we would see how terrorist groups in particular have built their own moral codes which enable them to adapt their own conduct egosyntonically to justify their own behaviour in psychological terms.[3] Thus, without indulging in elaborate lucubration, it is easy to see that criminal adaptability calls for the same proactive capacity on the part of the security systems in place to guarantee our limits (public freedom and citizens' security, according to the Spanish Constitution) for co-existence in an environment in which criminal organisations act as predators, albeit only to balance our capacity of response in view of their adaptability.

Considering security intelligence as a superstructural framework in a renewed approach by public security agencies, I would like to identify knowledge-based security as the foremost component of intelligent security. A number of traditional security schemas are based on the horizontal, widespread assumption that a particular system at risk (individual, corporate or social environment) must be protected by reactive armouring against a range of possible threats. This applies a linear doctrine of distancing, encapsulation, isolation of the security subject in respect of the threats posing a risk.

These traditional security systems based on physical barriers, on containing or dissuading threats, often completely ignore any analysis of the behaviour of the threatening agents, of the triple contextual layer (the context of the subject at risk, the context of insertion of the threat and the context of inter-relation between the threat and society or its agents when introduced in the security sphere), and of the characteristics and response capacity of the agents subjected to security. The foremost special feature of intelligent security is that it is based on knowledge of the entire configuration of elements which influence a specific security area.

Knowledge-based security intelligence is not the result of some metaphysical whim, intellectual modernity suddenly introduced into the sphere of security or a simple conceptual or academic coating which lends an air of sophistication to traditional security measures. Security intelligence simply cuts procedural and structural costs (it is efficient), on the one hand, and adjusts criteria between means and ends, reducing collateral effects by introducing accuracy and selection into the tools applied to achieve the objectives (it is effective), on the other hand. This is because security is subsidiary to thorough knowledge of the environment in which it operates.

Traditional security often does not take into account the analysis of the nature of the threat, and therefore its potential variations, and consequently it exposes the subject of security in the event of even the slightest change in the initial conditions. Accordingly, all we know about the threat is that it triggers a risk and could pose a danger, and all we know about the subject of security is that it is vulnerable and must therefore be protected by placing distance and obstacles between it and the threats posed to it, or eroding the capacity of the threats to actually produce risk.

[3] A. Montero, 'Ensayo sobre la mente de un terrorista', *Debats*, nr 91, 2005-06, p. 62-71.

Adaptive and Pro-active Security

Another property of intelligent security is its adaptability. At the opposite end of the scale from rigid, static and unchangeable rules, new security must comprise flexible, self-assessable systems that change in line with the interaction between the properties of the various agents involved in the security scenario. The aim is to achieve a system which can learn from itself, which is an intrinsic property of intelligence.

Adaptability is not the ability to react to a threat, to organised crime or to terrorism; on the contrary, it is precisely the ability to predict based on knowledge of the nature of the threats. Based on integral knowledge of the threat and its insertion context, and also of the nature and response capacities of the security agencies, tailored systems are devised which take into account the longitudinal development of the conduct of the parties involved. In order to make a security system adaptable, it is indispensable to provide it, first and foremost, with intelligence resources and, secondly, to attach prospective methodology to those resources.

The aim to build a system which can learn from itself is dependent upon including certain protocols for self-assessment in each security schema. These protocols, which may be implemented from central security bodies in a range of projects, must form a horizontal dimension of each security system. Accordingly, the security plan will ensure that each of the resources and procedures in place always respond to an assessed need, that they do not incur undesired dysfunctional effects and that they fit in with a permanent rationalisation of costs.

An evident example of the problems of adaptability in public and private security systems is the fight against terrorism. The use of a specific tactical system by a terrorist group in the attacks which stunned the United States on 11 September 2001 has translated into an irrational oversizing of security measures worldwide. This approach systematically ignores adaptive capacity which, in this case, does govern the conduct of criminal organisations and terrorist groups.

The widespread introduction of poorly-thought-out security resources in air transport is no doubt influenced by geo-strategic factors and high doses of politics. The fact that the Sarin gas attacks on the Tokyo underground in 1995, perpetrated by the Aum Shinrikyo group, did not translate into a multiplication of security systems on underground railway lines worldwide and, in contrast, 9-11 led to almost unanimous linear extrapolation of security methods at the international level, hints at the complexity of objective security and, especially, subjective security. Another trivial but hugely revealing detail is that the discovery of a crudely-designed explosive device in a passenger's shoes, related with international Jihadist terrorism, triggered an obsessive search for further threats in the shoes of passengers the world over.

These glimpses of old-style security in the face of new terrorism indicate, quite clearly, how planning is sidestepping comprehensive analysis of the nature (natures) of the terrorist threat, while at the same time hampering the implementation of preventive and predictive measures. There is no doubt that planners and strategists on the threat side are innovating, applying divergent thought, not to their doctrines but to their tactics, always seeking to open a lateral tunnel in the security systems in place to prevent or hamper their actions. All of our responses tend to reveal central alignment, whereas terrorism and organised crime move along lateral lanes.

To sum up, proactivity is a concept according to which, having analysed the potential threats in a particular environment and their possible future behaviour, actions are designed so as to modify this behaviour, anticipating the dynamic of the threat to reduce

the risks to a specific environment. Obviously, the more complex the threat, the more difficult it is to predict its behaviour and, logically, the harder it will be to implement a proactive response to minimise or prevent the underlying danger. Today, in what is already an intricate multipolar international reality, complex threats to our societies are closely linked to either criminal phenomena or international conflicts, both of which involve the presence of groups with hostile intentions, closed and exclusive groups and the quest for personal gain, in economic or power terms, which situate them above the law and above human rights.

The essential purpose of intelligence communities is to prevent threats; not specifically to investigate or suppress them, but essentially to pre-empt them. The articulation of methods of observation and investigation, analysis and interpretation, would be subsidiary to this horizon of prevention and avoidance of danger, threats and attacks: preventive intelligence.

Prevention of international organised crime or terrorism in the future will not hinge on security but on intelligence, or rather security emanating from intelligence. The British Prime Minister Tony Blair rightly summed up this approach by asserting that 'The one thing that we have learned post 11 September is that to take action in respect of a threat that is coming may be more sensible than to wait for the threat to materialise and then to take action'. The key, then, lies in prevention based on intelligence; in other words, on an adequate understanding of the dynamics of the terrorist phenomenon in order to proactively be one step ahead of it.

Prospective Intelligence for Security and Defence

In an attempt to articulate a conceptual framework, Bas[4] points out that 'the objective of prospective intelligence is to predict future variables (possible futures), assigning them an estimated probability (subjectively or objectively) and a degree of desirability (in line with starting objectives). Prospectiveness, then, based on past and present information and speculation in regard to the future, seeks to chart a cognitive map which will enable us to identify various options and reduce the level of uncertainty which is inherent to any decision'.

Prospective security intelligence is the use of knowledge for action on future risks, and on the present pattern or patterns leading to these future risks. Consequently, in security and defence there is no such thing as foresight without knowledge (intelligence) and there is no value if our early interpretation of the phenomena is not linked to preventive action. This prospective action may be strategic, as seen by most authors,[5] but also tactical, in other words, it is also useful to make headway in foresight applied to operations. At this point there is no avoiding mentioning preventive actions, especially in the sphere of defence, when following 9-11 one of the most significant and controversial strategic additions to the security doctrine of some countries became that of 'pre-emptive attacks'.[6] However, the concept of preventive proactivity in security should not be stretched to the point where it acts against citizens before they break the law, but should mean implementing security resources to reduce the opportunities –and this is where prevention lies– of criminals executing their plans to break the law in specific social contexts. Accordingly, it will be possible to articulate an integrated response to the global threat of

[4] Enric Bas, 'Prospectiva y prevención de la delincuencia organizada', Prospint Conference for Public Security Directors, 4/V/2005, Ministry of Interior, Madrid. See also Enric Bas, *Prospectiva*, Ariel, Barcelona, 1999.
[5] For a leading reference work see M. Godet, 'Prospective et stratégie :approche intégrée', *Futuribles,* nr 137, November 1989.
[6] F. Arteaga, 'La estrategia de seguridad nacional de Estados Unidos de 2006', ARI nr 71/2006, Elcano Royal Institute.

organised crime encompassing all the potential and resources of security services and police.

The development of prospective intelligence capabilities is a territory with huge potential in the security forces and it is an interesting area for research and refinement by analysts. It is true that the analysis of risks which, for example, is being applied in the control of persons and goods in airport facilities, or in introducing profiling components in the analysis of financial information relating to money laundering, are promising starts in this area. However, prospectiveness is still far off and it would be highly inefficient in the absence of ongoing work to improve the quality of the process of data analysis, especially concerning the development of rigorous and homogeneous information processing systems in State security forces and, most especially, the architecture of a specific methodology for strategic analysis of information and output of intelligence for strategic decisions in public security.

Descriptive Detection and Assessment: The First Axiom of Prospectiveness
In regard to what we might define as the first axiom of efficient prospectiveness –data processing–, in future studies we must be aware that the indispensable groundwork is a thorough description of the phenomenon, the area of knowledge, from which future patterns are to be built. In terms of security prospectiveness, it is clear that the knowledge that is hardest to compile is not to do with the future, but the present. This is true to the extent that if we had an accurate description of the variables, factors or components involved in a specific security phenomenon (which might be strategic, such as the development of Jihadism in Spain or more operational such as the activities of a stable criminal group involved in trafficking human beings), the influences between these elements and the conduct of each element individually and in relation to others, and if the knowledge schema also included all of the sufficient and necessary components to make the phenomenon materialise, with neither too many nor too few, then forecasting would be automatic, it would be a prediction, a predictable future. The disadvantage of security prospectiveness vs. any other sector or general prospectiveness, is that nothing happens in such a deterministic way.

Prediction tools operating on quantitative data work well, but we are not able to adequately operationalise most of the variables and, when we do make a satisfactory guess, we are likely to have left out of the prospective equation some factor of causal influence which we have not even detected. The most important and complex issue in projecting future situations is to detect and assess current variables: in that order, detect first and assess later. In security, most of the components to determine the performance of a phenomenon are social, more specifically human. Social sciences or psychological methodologies have made considerable progress in recent decades and have managed to include multivariants which entail a series of factors, categorise them and prioritise them, to offer a quantitative profile of the subject under study. However, as experts in behavioural sciences well know, despite attempts to operationalise and quantify the human personality, we are still unable to accurately describe, using only psychometric instruments, an individual's conduct. The efficient analysis option is to integrate this quantitative result into a qualitative method of interpretation. However, even if we had developed reliable qualitative systems –which we have not– the thorough detection and accurate assessment of factors is still inevitable.

Accordingly, basic conditions for prospective security intelligence aimed at transcending more or less literary speculations are, first, that the focus of the analysis must include social variables, to offset the traditional tough security factors (confiscations, attacks, how many weapons, how many crimes, etc.), and, secondly, that the prospective-security analyst must have access to information on the variables, factors and elements of a structure, situation or group to be studied. In other words, taking macro-, meso- and

micro-approaches and having elements of observation and detection that are sufficiently refined.

This position translates into the fact that, when we try to approach prospective analyses on organised crime or terrorism we will have to think beyond the specific criminal phenomenon, especially when the subject of our analysis is strategic. Prospective security studies may be applied to the evolution of a terrorist group, in order to anticipate its behaviour. Researchers from anti-terrorist units are painfully aware of how difficult it is, especially considering all the constraints in terms of time and security surrounding work to dismantle terrorist groups. However, if someone with access to all the field data during the two years immediately previous to 9-11 and 3-11 (and access to all the operating information means without compartmentalisation by agency, which fragments and adds bias to an analyst's interpretation), if such a person had been able to tie together the pieces of information and had contextualised them in line with social aspects, perhaps the public security institutions would have had a better chance of predicting events. Nevertheless, it is doubtful whether, even having total access to information, detection and observation of the suitable variables for prognosis would have been optimal. The prospective security analyst should always ask whether he has all the variables on the table, whether they have been well catalogued and compiled, or whether more investigation is needed to make future projections. And this is the second axiom of prospective security intelligence: method.

Specific Methodological Architecture for Strategic Security Analysis
The cornerstone of foresight is observation. We observe, we detect, we assess and we catalogue. Then, we assign weightings of influence, we link and we project. The inaugural guarantee of any unit of prospective security intelligence is to have bodies for obtaining information which contribute direct lines of knowledge in regard to the phenomenon under study. These live information channels, which in most cases have a security classification (they are confidential, reserved or secret), in prospective analysis are contextualised with contributions by open sources of information. It is not sensible to imagine creating prospective intelligence units without having at least a micro-department to process information from open sources, which in the case of strategic analysis should be guided observation, with clear set patterns, although without relinquishing flexibility.

Now, assuming an ideal prospective department with access to both classified and open information, the next step in the methodology is to ensure that the focuses of our observation are in line with a sufficient range of detected variables, in other words, that we consider the right questions and that we focus on key variables. From an instrumental standpoint, to attain these ranges of variables, prospective study tends to use structural analysis.

To simplify, structural analysis consists in starting by cataloguing a phenomenon's central core, and the factors and elements of which it is comprised, without entering for the moment into its causal or correlational interactions, but establishing links between the system's components (for now all we need to know is that a particular element is linked to another, and we can leave ascertaining their relationship of influence for later investigations). In regard to the interconnections, which will later shape our 'map' of the influence relationships between variables, something which tends to be obviated when a structural analysis begins is that the prospective analyst should have a theory about how the phenomenon works. This is exactly what happens in scientific research: it is the theory which sets the pattern for compiling data. It is not necessary to underline, therefore, the significance of the fact that future prediction teams must not be little more than meteorologists, with no contact with the disciplinary area of applied knowledge (it is impossible to make predictions on international Jihadism without seeking a specialist in

the matter or unless the prospective team comprises a combination of conceptual experts and methodological experts).

The floor on which structural analysis is built is the exercise of making emerge the variables, to which task a future prediction team should devote whatever time and techniques (brain storming, etc.) are necessary. It will be seen later whether or not these identified variables on which the future projections will focus are quantified or quantifiable, and whether or not we have adequate descriptions of each of them (descriptive statistics, in quantitative hypotheses). Accordingly, the use of variables is the linchpin at this stage of creating an analysis matrix, and it is so significant that it inexorably shapes the future predictions to be built.

Some prospective analysts perform structural analyses exclusively via quantitative procedures. Normally some kind of exploratory factor analysis is performed. This is a mistake. Reductionism in studies on the future is the surest way to make a mistake in a projection. In security sciences, as a discipline of social sciences, phenomena are multivariant and many of their constituent elements are qualitative or, at least for now, are factors that are difficult to operationalise. Exploratory factor analyses are an excellent basis on which to begin to build structural analysis, but they are a minefield of interpretative bias if they are used as the only channel for developing a futures projection.

On the opposite side of the positivist paradigm which prevails in our science, the quantification of variables is, following the detection of these variables, the Achilles Heel of prospectiveness. So much so that, with the major advances in mathematical sciences and statistics in convergence with information technology in recent decades, economic experts are still unable to make predictions with minimum uncertainty in regard to the evolution of stock market securities. Granted, we do have countless predictions on the performance of economic and stock market values, but it is no less true that no consultant will guarantee that our investment in a package of listed securities is only going to rally. They do not, because, despite being quantified values, there are other social variables (not quantified and, to make matters worse, not even detected and envisaged by econometric models) which explain why, at a specific time, there are sudden oscillations in some securities.

Structural analysis precedes and complements morphological analysis. In fact, we would do well to recall that they are actually two stages of the same kind of analysis, devoted to first establishing the molar configuration of a problem and to later break it down into its molecular components (its morphology). The construction of a morphological area consists in schematising the possible combinations of which each factor identified in the structural analysis is comprised. It is a detailed exercise, where those constituents of structural factors are derived, combining them with various possibilities with meaning for each factor. To draw a parallel with trying to make a prospective study of an individual's behaviour, structural analysis would consist in building a repertoire of factors which determine that behaviour (from social, personal, employment, family, even personality factors, including character, constitution, intelligence, etc.), whereas morphological analysis would be an attempt to break down these structural factors (for example, employment factors are broken down into the person's post, responsibilities, track record and the various possibilities and influences of each of them; personality would be broken down into the person's traits, character in attitudes and intelligence in cognitive response styles, etc.), looking for the various probable combinations for each of these elements resulting from the breakdown. The more thorough the morphological analysis, the less uncertainty when it comes to future projections. Once again, if we are working with operationalised and quantified variables, an exploratory factor analysis would reduce the main components of each factor. However, in security phenomena this is anecdotic if we aim to encompass the entire structural space, although it is feasible to use this statistical

process for some of the variables of the problem submitted for study which we have suitably measured and converted into figures. Morphological analysis contributes theoretical solutions which can later be polished by a combination of quantitative instruments (confirmatory factor analysis, neural networks) and qualitative instruments to channel future scenarios.

In combination with morphological analysis aimed at modelling scenarios and future possibilities, foresight analysts are resorting increasingly to three types of mining: data mining, text mining and web mining. Mining looks for underlying links between pieces of information. It is important not to confuse mining with information retrieval. Based on the meaning of the word 'mining', applied to information processing, it is clear that the purpose of these techniques is to hit a useful 'seam' among the 'rocks'. When we talk about information, mining helps in the task of finding precisely that information which, although present in a volume of data, is not directly visible to analysts. These 'seams' of information, when dealing with numbers, texts or websites, almost always refer to items of information which emerge during mining when, via that process, links are established between information elements which are visible to analysts *a priori* (the 'rocks'). Evidently, mining is useful in any segment of the information process, whether operational or strategic. It may even be applied prior to the construction of a theory or model of reality by the analyst (in other words, before or during the structural analysis) in order to find substantive indicators to shed some light on interpretation.

Following these phases of analysis, the interpreter of information devoted to prospective security will be in a position to model scenarios, to build reality models. The scenarios can be reached based on a Delphi study or in combination with the aforementioned analyses. What is unavoidable in the construction of future possibility hypotheses is the consideration of central, proximal and distal variables which influence the behaviour of a problem and identification of the way in which they relate to each other so as to determine that behaviour as it is manifested. The various predictable evolutions of these variables and their relations are what comprise the possibilities, in other words, the range of scenarios which the analyst will propose to the decision-maker as possible routes of future development.

In a methodologically consistent prospective study report, a number of future possibilities must be set forth in order to trace the evolution of the subject of a study. At least three scenarios are normally devised:

(1) Tendencial or Baseline scenario, which comprises the most plausible assumptions on the performance of variables and which basically coincides with the theory which the prospective analyst uses as a model of the reality which he is studying, as we have already mentioned.
(2) Contrast scenario is a probabilistic variation of the tendential scenario and allows the possibility of performance resulting from the core variables of the phenomenon being subjected to different kinds of influences. Contrast forecasting is the exercise of alternative thought, where the analyst must consider the range of 'looseness' of some of the variables involved to trace what would happen if (the trademark *what if* in prospective studies) certain ingredients of the phenomenon were to trace a different course of behaviour. Some authors consider that the contrast scenario would be the future possibility which would show us what would happen in exactly the opposite event of what the tendential forecast says will happen, so that the contrast would serve as a kind of 'insurance' in the decision-making process (along the lines of 'I am going to consider the opposite outcome just in case').
(3) Prescriptive scenario, which would be equivalent to placing, within the scope of the problem which we have defined, the focus of analysis on variables linked to the security institution performing the study or security bodies of a country or government

or, in short, the players who would take the actions linked to the prospective study being performed (if it is a prospective study about Spanish foreign policy in Morocco which is being performed by Elcano Institute, for example, the prescriptive scenario would explore how a specific action by Spanish institutions and companies could model a specific future possibility and, therefore, what that future possibility would be like). This is the most interesting scenario for prospective security intelligence and it is where public institutions should commence work. This future possibility is concerned with whatever, as a society and via our specialist institutions, we can do to prevent a particular risk scenario from developing or materialising. It is, therefore, the scenario which enables us to avoid reaching the point of having to take drastic measures, such as pre-emptive attacks or similar actions, since it builds the future picture based on the present and using our diagnosis and our intervention in regard to the diagnosis. Naturally, the prescriptive scenario is as difficult or more difficult (since it involves knowing our organisations very well and including them in the analysis, avoiding prejudices and indicating each of our defects and limitations) to model than the previous ones.

Based on this minimum, as many scenarios can be built as the elasticity and rigour of the analysis permit. Indeed, the scenarios tend to be given names to label the future possibility to which they refer (for example, 'black scenario'[7]). At all events, it should be standard practice in prospective studies to consider the alternatives and, systematically, various different future possibilities. Absolutely deterministic predictions do not exist, for now. This is especially true for prospective studies on security, which on the one hand is so dependent upon social variables, and on the other is so constrained to the decision-making process so as not to allow too much speculation due to the impact on people's lives. Reports on prospective studies of security intelligence, as well as offering a clear picture of the range of possibilities, should include gradation of uncertainty, and be scaleable in their treatment of knowledge.

Grading uncertainty means introducing a sequence in the drafting and exposition of the prospective report which should make very clear to the product's consumer what information the analyst knows for certain; what portion of the product corresponds to a description of the phenomenon; what portion explains it; what portion proposes a hypothesis; and where the tracing of future possibilities begins (and where possible, the associated probabilities should be set forth). This will tell the persons whose job it is to decide which degree of uncertainty they are accepting by adopting a particular decision possibility and on which elements of analysis, from the most to least certain, their decision to act is based.

The construction of scenarios has, without doubt, the objective of proposing future possibilities for decision-making, but there are others. Performing prospective analyses will substantiate much of the activity of a futures department, but it will be an activity with no future of its own (to use a play on words) if it is not accompanied by another purpose, which must be maintained by prospective staff: namely the construction of profiles with early-warning indicators. The construction of early-warning indicators is an activity aimed directly at actionable prevention. It consists in finding markers which forecast the presence of a phenomenon, factors whose emergence, while not in itself a threat, normally precedes a threat, or elements which, once they have emerged, will eventually lead to a risk situation.

[7] An exercise of this type, although without probabilistic pretensions, can be found in C. Alonso Zaldívar, *Invasión de Irak: escenarios negros*, Working Paper, 14/I/2003, Elcano Royal Institute.

Departments of Futures in Security Institutions

A number of conclusions may be drawn from the investigation commission set up in the United States to clarify, as far as possible, the nature of the response by public powers to the terrorist attacks of 11 September 2001.[8] In terms of our reflections in this Working Paper, two of these are particularly significant: (1) the need to find vertices of convergence in information processing, so that at least one interpretation group may be in a position to assess threats with useful and actionable information, resulting from adequate coordination between security agencies; and (2) the need to improve our interpretation of the threat based on analysis of this information.

In respect of the first conclusion, creation of the Homeland Security Department and the appointment of a National Intelligence Director in the United States, or the institution of the National Centre for Antiterrorist Coordination (*Centro Nacional de Coordinación Antiterrorista*) in Spain, are steps, albeit slow and modest, towards congruency. In regard to the second, training public security professionals to interpret in a more efficient and preventive manner the complex threats to citizens, the response has included the creation in the United States of the Sherman Kent Center for Intelligence Analysis and the creation in Spain of the Intelligence, Strategy and Prospective Studies in Public Security, the socalled Prospint programme.[9] Both initiatives seek to develop doctrine and equip public security analysts with skills in methodologies to interpret complex realities which transcend rigid and self-satisfying schema in approaches to security threats. In other words, to learn to manage uncertainty.

The Prospint programme also envisages the development of analysis and interpretation methodologies which provide a Spanish community of intelligence analysts with the tools to undertake prospective strategic diagnosis. The ultimate aim is to combine public capacities for obtaining information with a better interpretation to build models which enable decisions to be made on criminal realities when they start to cause the very least damage. In this quest, obtaining information is as important as accessing and interpreting it. There is no use in having sophisticated satellite systems to obtain information if our analysts interpret the data against a backdrop of institutional fears, information processing bias or deficient skills in terms of methodology and reasoning.

For now, in Spain, prospective security intelligence is, in itself, a future possibility. There are only a few professionals at institutions, such as the Office of the Secretary of State for Security, the National Intelligence Centre (CNI) or the army's MADOC command for military training and doctrine, which have either been working sporadically in this field for some time without much organic or functional impact, or are just setting out in response to a certain will to provide this training on the part of directors. The fact is that the plans for 'units of futures' –which would be the most appropriate name, with the "futures" in plural to avoid determinism– or full-time prospective studies services to develop anticipatory or preventive analysis lines is much simpler than it looks. We have to stop thinking in bureaucratic terms and start taking a functional and flexible approach. To start with, on a full-time basis, no more than two professionals are necessary per institution, with the capacity to build temporary ad hoc work teams.

Both structural and morphological analysis, and the subsequent tracing of scenarios, should be planned and developed as a team. The feasibility of a lone analyst performing these stages of prospective studies is highly doubtful. Since they are phases whose purpose is to describe the nature and detailed composition of a complex problem, one is

[8] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* W.W. Norton, New York, 2004.

[9] Prospint is a programme run by the Secretary of State for Security within the Spanish Interior Ministry, managed by the head of its Analysis and Prospective Studies Department.

unlikely to come across an individual analyst who, having determined the problem, is able to produce a wide repertoire of variables while avoiding his own theoretical bias and processing errors; one with a volume of knowledge so as to be able to build, with no contributions from others, a theory on the guiding operation of the analysis and who is also an excellent methodologist and familiar with the necessary instruments. As well as being unlikely, it would be inefficient.

Futures or prospective units are horizontal entities, in other words, they should be applicable to the study of any security problem. Accordingly, they should be organised around teams with a stable core but with flexible perimeters. The combination of staff units and task forces is ideal: a unit that is a part of intelligence or operations directorates with a staff of two professionals, one of whom should be a director of teams with advanced knowledge of analysis and knowledge of prospective studies, acting as orchestra leader in each study that is performed; and the other a methodologist, who will contribute scientific and instrumental rigour to the analysis. These two figures will be perfectly positioned to build the staff of a futures unit to start producing prospective security intelligence. However, although necessary, they are not enough to undertake prospective analysis. For each commission, a task force should be set up with the following components: one or two specialists in the area under study (for example, Jihadist terrorism or trafficking of human beings) and one specialist in information processing and analysis. For each study, intelligence and operations directors should afford the necessary security authorisations (this is not the custom in Spain, but it is bound to change since we have no choice).

Conclusions

Democratic societies are no longer only clamouring for public powers to arrest and impose sentences on terrorists who have committed attacks: they also demand that security institutions financed by taxpayers be in a position to know the threats and, based on that knowledge, prevent a planned terrorist attack from ever being carried out. Not only that, but, if possible, democratic freedom demands that organised crime not be allowed to overrun certain areas so as to reduce citizens' well-being. In view of this preventive approach, police forces and security agencies have no choice but to develop intelligence bodies which build on knowledge and forecast the behaviour of threats. It is not enough to obtain information from inside and around every threat, but it is necessary to process the information and interpret it, to decipher the threat, to devise reality models which permit preventive action. After years of progress in information analysis, security agencies must now be prepared to undertake forecast analyses of reality, to enter the realm of scientific conjecture, of the construction of futures. This journey, which calls for a major change in the reactive culture of security organisations, has only just begun.

Andrés Montero Gómez
Coordinator of the Prospint Programme of the Office of Spain's Secretary of State for Security