20th ICCRTS

I - 100

Title: **Thoughts on Danger, Risk, and Threat**

Topics: primary: Topic 1: Concepts, Theory, and Policy
alternate: Topic 2: Organizational Concepts and Approaches
alternate: Topic 4: Experimentation, Metrics, and Analysis

Name of Author: Mircea MOCANU, PhD
Author's affiliation: none, retired, former military intelligence officer.
Author's complete address: Bucureşti, Str. Conţeşti nr 6, bl P-83, sc 1, ap 19, sector 5, ROMANIA.
POC Name: **Mircea MOCANU**
POC Organization: none, retired.
POC Complete Address: Bucureşti, Str. Conţeşti nr 6, bl P-83, sc 1, ap 19, sector 5, ROMANIA
POC Telephone: + 40 734 690 176
POC E-mail Address: **mirceamocanu@yahoo.com**

Abstract: Danger, risk, and threat have numerous definitions in various domains. However, not enough generally accepted clarifications of these concepts are available. Considering danger as event causing a negative effect, its objective elements can be calculated or estimated. The subject identifies danger and develops a perception on the elements of danger, based on its interest. Subject's decision about an action introduces the human factor, and its subjectivity, when the subject establishes correction coefficients for the elements of danger, and a relevance for the danger. Thus, risk is an interaction between subject and danger. Threat appears as a type of risk, where a hostile entity intends a hostile action against the interest of the subject. Opportunity and vulnerability are also discussed.

Risk management is the subject's activity regarding danger, which is a complex enterprise, with psychological components. A difference in the meaning of risk in intelligence and risk management is highlighted, pointing to the difference of roles between the two parties - the epistemic role of intelligence vs. the deontic role of the decision-makers.

The conclusions support different levels of expectation for metrics in Command and Control, due to the different meanings and contents of human factor in danger, risk, and threat.

Key words: danger, risk, threat, risk management, security environment, Command and Control.

I - 100

Thoughts on Danger, Risk, and Threat

COL (RET) Mircea MOCANU, BE, PhD*

Numerous domains include risk management activities. However, there are various aproaches and many definitions of the basic terms in the realm of risk. The present growth in complexity and interdependency provide the reason to sort through that chemistry and to harmonize the notions and concepts utilized in practical activitites albeit simple or of the highest social importance.

1. Danger

In principle, as a primary element in risk theory, DANGER is the negative aspect which can define the postion of an actor / subject within its environment, which may include undesirable elements or developments. As a fundamental element, Danger appears in the international security environment, in the political, military, and economic spheres, and embraces activities spanning from armed conflict, to normal everyday life, including sports, games, and gambling.

Knowing that the negative *effect* works either suddenly, at a certain moment, or distributed over a period of time, Danger should be considered in its dynamic dimension, i.e., as an *action* - one time event or a development. Before an action presumed to have a negative impact actually happens, the generating element of that action presents the capacity, the ingredients which make it *dangerous*, able to produce Danger. Yet an inert object, a phenomenon or an inactive person cannot be a Danger in itself, in the absence of an action entailing a negative effect within the considered environment, henceforth called *Security Environment*, writ large. The capabilities which can generate negative effects present the potentiality for Danger and can be observed and measured. However,

* COL (RET) Mircea MOCANU, BE, PhD, has worked as head of Analysis, Military Intelligence, Ministry of National Defence of Romania, and head Production Branch, IMS INT Division, NATO HQ, Bruxelles, Belgium.

Danger is really present only when an undesirable *action* - event or development is triggered. We have in English the expression "an accident waiting to happen".

In the classic culture there is the expression "Sword of Damocles", where not the sword itself is the Danger, but its fall on the head of Damocles. Maybe a better example is the basic principle in martial arts, where the force of the enemy is not itself a Danger, but the action in which that force is used against the fighter. This is why the fighter exploits the force of the adversary to counter the Danger to become its victim. Thus, the force of the enemy becomes a useful tool to reach security, instead of a Danger.

The realism and utility of this observation are obvious in the practice of prognoses, where the forseen Dangers are actions or dynamic phenomena, not inert objects or inactive individuals.

But Danger does not apply only to future actions, but to past actions as well, if the negative effect has not been perceived yet by the interested actor, or, in other words, if their impact has not yet inflicted the Security Environment as it is defined. In this case, the actor takes into consideration the posibility of a past action about which he has no knowledge if that action occured or not, because he has not suffered any impact thereof. For example, "I am not sure if I locked the car door. It is possible that somebody would have already stolen something from the car, or the car altogether"; Or "The customer does not answer the cellphone. Should he have forgotten it at home, we won't be able to talk the whole day, and deal is lost".

The negative effect / *Impact* of the event considered as Danger can be expressed by various units measuring *Loss* (hence, the parameter is denoted as *L*): money, quantities of goods (e.g., tones of wheat), time units, victims, symbolic tokens or points (in games), land surfaces, depreciation of health situation, politic support, media rating, etc. More difficult to express are the abstract losses such as prestige, national sovereignty, personal affection, social position, liberty,

membership in various organisations or structures (for example, the danger of being excluded from an alliance, a club, a gang, or a political party).

Associating Danger to an action points to the *time* perspective, either the moment of occurrence / incidence of the undesirable event or the duration of its performance. Regarding the moment of incidence, a parameter called Urgency can be used, denoted as U and defined as a function of the time difference available from the current time t_0 to the (known) moment of incidence of the undesirable event t_l, so $\Delta t = t_l - t_0$, and $U = 1/\Delta t_l$.

The other time parameter specific to the action of Danger, *the duration of the negative effect*, works in other ways than the moment when the action starts. More precisely, the duration of the negative action defines the effect in terms of costs or other loss values, rather than in terms of time units linked to that action.

Further on, the objective character of Danger and the measurability of the Impact and moment of incidence lead to the need to consider another parameter of the undesirable action to reflect, nevertheless, the uncertainty of the material and social world. That is the likelihood, or *Probability of incidence* (designated p_l) as of the undesirable event. For dangers specific to the physical world, such as the probability of a bridge colapsing under a certain weight, the impact and time of incidence, but also the probability of occurrence can be measured by mathematical methods applied to physical phenomena - which is perfectly normal. The problem appears in the case of dangers of social nature, mentioned above, where the human factor is involved, and the measurability decreases while the uncertainty increases. Here, the Loss / Impact, the moment and the probability of incidence can be estimated, at least vaguely, with a probability and margin of error, according to the laws of statistics and system theory.

Consequently, three parameters are identified - Impact (L), Probability (P_l), and Urgency (U) - all calculable by mathematics or at least estimated by reasonable models and logics, considering certain assumptions. These

parameters point to the objective and measurable character of Danger, with limitations regarding the probability of incidence.

A combination of the three parameters should provide the primary integrated expression of Danger. Since Danger is practically null when any of these parameters is void, the best form of its expression should be a product. A good example of a Danger having a negative impact of cataclismic dimension and very high probability of incidence, yet irrelevant because of the distant moment of incidence, hence almost null Urgency, is the Danger that the Sun shuts down. It is a certainty that does not concern us because Δt_l is huge, which makes Urgency (parameter *U*) almost zero. So, the expression of Danger should be

$D = L \times p_l \times U$,

where *D* is the value associated to Danger, *L* is the value of Loss or Impact, p_l is the Probability of incidence for the loss / impact (objectively calculated), and *U* is the Urgency, defined above.

In this form, the expression of Danger provides a measuring unit *cost*/*time*, which does not offer a universal utility, but only a utility limited to the comparison between similar dangers, having the same type of costs: money, number of victims, damaged surfaces, even time, or abstract values.

The product form proposed here to express Danger yields an exponential range of results, a dispersion of values. This is a practical advantage, because a dispersion of values is useful to better rank dangers, and discriminate the mitigation, prevention, and countering of various kinds of dangers.

2. Subject

The issues presented above point to the fact that Danger only makes sense when linked to an actor or SUBJECT who would suffer / receive the negative effects of the undesired event, who would perceive the negative shade on that action. At this point, the originator / cause of the undesired event is not relevant.

The Subject is easy to understand; However, some considerations are worth making. First, only the criteria used by this player in the security environment realities are those which establish the *negative spin of the action* which, this way, is judged as Danger. For other actors, exactly the same action may be indifferent or even gladly received, and not at all a Danger. A good example are the zero sum games, the card games or the board games.

Getting the Subject into the equation brings along features proper to the human factor, hence the value of the psychology point of view. The first contribution of the Subject is, of course, the *subjectivity* of the relation, its dependency to the Subject's evaluation. Subjectivity appears as soon as the *identification* of the negative character of the considered action, because, as mentioned above, another subject, in the same environment, may judge that the considered action is not a danger, maybe even on the contrary. So, the Subject is the one to decide if an anticipated action is a Danger or not. This no-brainer is based on Subject's *perception* on that action. The perception pops up quite quickly, even before any calculation of the impact and moment of incidence. On the other hand, the Danger identified by the Subject may be a part of a bigger Danger, having a larger Impact, yet not all affecting the Subject, but only a part of it. For example, the perspective of a fall in stock market may loom over a large number of individuals, but one individual Subject, who is concerned only about his limited investments, may consider such Danger as insignificant.

The animal kingdom demonstrates that perception about Danger can be even integrated into *instinct*, which appears, here, as an integrated and automated identification form for the negative character, and a quick estimation of loss, urgency, and probability of incidence of the negative event.

Due to its subjectivity in approaching the Danger, the observing / receiving Subject brings its own interpretation regarding the Danger, *D*, and makes an adjustment which the author denotes as *Relevance*, which will be discussed later.

By the Subject's perception about the negative character of the impact, as well as about the parameters of Danger, the human factor highlights another feature of the Danger, that is *uncertainty*. Uncertainty looms over the relation between Subject and the security environment, even since the "grey period", when the study of various security environment realities does not yet lead to decisions regarding the negative character of possible actions. The Subject acts to diminish uncertainty by *observing* the Security Environment, but the "birth certificate" of the idea of Danger is the very *establishment of the negative character* of the possible action / event.

During the observation of the Security Environment, the Subject can detect events that can negatively affect the interests of other entities, not his. As long as these phenomena or events do not have a direct relation with the Subject, they only contribute to knowing and understanding the Security Environment. As the Subject develops various relations with the entities jeopardized by those events, the rapport towards the Subject's interest can change, and the negative event can become a Danger for the Subject, or, perhaps, an opportunity.

On the other hand, one should notice that the Subject can be individual or collective. In the case of a collective situation, the Subject can be a family, a group of persons, a firm, a battalion, a nation, an aliance, the United Nations Organisation, or the whole mankind. For the collective subjects, the relevant feature is the *coherence* in perceiving the negative effects the group might suffer, the impact that certain external unfriendly elements can cause. The common vision of these effects defines the collective subject in its relation with the environment considering its common needs. Depending on this, the collective subject can be treated as an individual subject, as a sovereignty with a sole vision, will and action or, on the contrary, can be broken down to separate sovereign Subjects having separate visions regarding the negative effects generated by the considered Danger.

From the point of view of Abraham Maslow's pyramid of human needs, the negative impact of an external action can be considered on all levels of the hierarchy, from the physiological needs and the need of safety to the need of spiritual fulfilment and self actualization. Thus, the negative impact can be: the deprivation of physiological needs (starving the inhabitants of a beseiged castle, or "I won't be able to sleep because of neighbours' party tonight"); jeopardizing security ("Help, he's killing me!" or, in a military operation, the perspective to lose an asset of operational importance); a material loss (theft or damage), even moral damage ("Should he do that, he would shame us all!"); or, spiritual damage (insult towards Islam, blasphemy).

It should be said that a negative action can impact even a projection in the future, a perspective gain or chance, a hope, an ideal, a favourable future development, based on a program, an intention, a strategy, or a national policy.

The diversity of forms of impact is obvious. This is why it is useful to use a quite general term, and I think a good term would be INTEREST, a term which can describe both concrete values (of material nature), and abstract values (of nonmaterial mature), both of them with temporal characteristics of past, present, or future.

In the whole economy of risk, from the point of view of the Subject, it is necessary to explain Interest as accurately and pragmaticly as possible, and to express the value of Impact quite precisely, even mathematically, in order to eventually measure the Danger. Of course, in the case of a collective subject, a harmonization / consensus upon the Interest is paramount. These are the mathematizable aspects regarding the Subject, which are necessary to pursue practical solutions for the problems caused by various dangers. These solutions include making assumptions, identifying courses of action, making decisions, all activities pertaining to Command and Control.

A last but very important aspect regarding the Subject points to its passive or active attitude towards Danger. This approach manifests itself via three types of situations of interaction between the Subject and the Security Environment:

- The Subject can be passive, just an observer of the Security Environment and of the action identified as Danger. Such Subject has an epistemic authority;

- The Subject can be active, performing an action according to his intentions and unrelated to the identified Danger, yet in the situation to be affected by that Danger. Such Subject has a deontic authority; or,

- The Subject can be active, performing an action or a long activity conceived on purpose to counter the identified Danger - deontic authority as well.

3. Gain and Opportunity

Of course, the Security environment also includes phenomena and actions with a positive effect in the sense of Subject's Interest. This is why, in the mirror, the positive Impact of an action can be termed as GAIN (denoted as *G*) instead of Loss, as a punctual or continuous benefit, with a calculable or measurable value, consistent with Subject's Interest.

Also in the mirror, the above mentioned elements can be considered for the favourable sense of the evolutions in the Security Environment. In a similar way as perceiving Danger, the Subject perceives evolutions, situations or circumstances having a positive potential, which offer the perspective of actions that can generate Gain. Such circumstances are called OPPORTUNITY of Gain (denoted as *Op*). Similar to Danger, Opportunity is conditioned in time and has a probability (p_g) associated to the occurence of the favourable event. This is why, mathematically, Opportunity can be expressed as

$Op = G \times p_g \times U_g$, - similar to the expression of Danger,

where *Op* is the primary value associated to Opportunity, *G* is the value of Gain, p_g is the probability of incidence of Gain (objectively calculated), and U_g is the Urgency of Gain, discussed above. Urgency has a temporal representation

as a function of $\Delta t = t_g - t_0$, i.e., the time difference between t_g - the moment of incidence of the favourable action, susceptable to generate Gain, and $t_{0,}$ the current time.

4. Risk

With the identification as Danger, the interaction between Subject and Danger starts as a specific relation, where the observation of the Security Environment steps beyond the calculation or estimation of Impact and moment of incidence, to now include judgements regarding the precise ranking between good and evil.

The rapport and interaction between Subject and Danger within the Security Environment embraces a series of relevant issues: uncertainty; anticipated negative character; pursued Interest; the importance of both Impact and moment of the undesired event; the general evaluation of the Danger by the Subject (its Relevance); as well as, the Subject's attitude towards the Danger (action or non-action). These issues lead to defining Risk as a *situation or condition embraced by a Subject having a rapport with a Danger in a passive or active way, in view of a held / protected, yet jeopardized, Interest of the Subject*. The simplicity of this definition offers the advantage to open the avenues for specific adaptations in various domains, not only in security.

Risk cannot exist outside the two basic elements, Subject and Danger, and is fundamentally subjective. Considering an absolute risk is an error, because the Danger quotient (perception of danger) typically more or less changes up or down, depending on the historical experience level of the Subject.

So, the uncertainty regarding the Danger brings along the importance of Subject's perception, working through an objective measurement of the Danger (as objective as possible). Regarding Risk basically as a relation between Subject and Danger, and considering Subject's attitude, *subjectivity* works upon all the components of Danger, even if they are mathematically calculated.

First, regarding the Impact, for example, a certain loss in gambling, measured in a precise money value, can be considered less important by the gambler than by his wife. (Do you know the feeling?).

Secondly, the *probability of incidence*, which is approximative by definition, is regarded many times distrustfully and is corrected arbitrarily by the Subject. Again, gambling offers the simplest example: all participants to a lottery adjust upwards their own probability to win the big prize. Lotteries count on that. Otherwise, logically, based on the objective value of the winning probability, nobody would ever buy a lottery ticket. (Does this sound familiar?)

Probability is also a component of Subject's perception about Danger, included even in the first shape of this relation, that integrated into instinct. It can be agreed that probability is associated to Danger immediately, almost instinctually, in the moment that the negative character of the Impact is identified.

When subjectivity comes into play, the calculated or estimated impact (with a certain trust), and having a moment of incidence either certain or considered within a certain rush to action, the probability of incidence remains the most sensitive parameter of the relation between Subject and Danger. This is why, in a large proportion, the probability of incidence describes Risk as a whole, hence the temptation to define Risk simply as a Probability.

Thirdly, even the time available until the Danger strikes is corrected by the Subject. The author offers an example in another domain, not much different from gambling: the sincere vows of eternal love. (Maybe this rings a bell...)

These corrections can be materialized in coefficients attributed to the three elements of Danger, for example α for Impact / Loss (represented by L), β for Probability (represented by P_l), and γ for the Urgency (represented by U). Thus, the expression of Risk - R, based on the expression of Danger, becomes:

$$R = \alpha\, L \times \beta\, p_l \times \gamma\, U$$

Another aspect of the relation between Subject and Danger is the *intensity* of this relation, due to a stronger or a weaker connection between Subject's

Interest and the identified Danger. The intensity of this relation becomes another measure of Risk. From a different point of view, the intensity of this relation can generate various important attitudes and feelings for the Subject, such as responsibility, systemic concern, worry, caution, fear, panic, but also daring and courage, some of them discussed even by Carl von Clausewitz in his masterpiece "On War". The intensity of the Subject - Danger rapport, defined here as being the Risk, can be reflected by a new parameter which would combinee the three coefficients of subjective correction. I term this new player *Relevance* of the Danger, introduced already. This Relavance, noted with ρ, is the product of the three importance coefficients attributed to the three elements of the Danger. So, the Relevance noted ρ can be expressed as

$$\rho = \alpha \beta \gamma$$

After a Danger is *identified*, all of the above lead to the *definition* of Risk by the Subject, where subjective components generated by Subject's perception are added to the objectively measured elements of Danger. It is worth mentioning that uncertainty can generate an intense interaction with the Security Environment even without a clear description of the Danger, only based on a vague perception of Danger. It is the case of *fear of the unknown*, the simplest example being the fear of darkness.

In the same time, the intensity of the interaction between Subject and Danger, the instinctually attributed probability and the preservation instinct generate a strong association, near confusion, between the terms Danger and Risk, in the case of a passive Subject. This confusion leads to the temptation to over-mathematicize Risk, with expectations close to the calculations for an objective Danger. Also, the confusion between Danger and Risk makes the pragmatic approaches more difficult in risk management, by generating fuzzy concepts and arbitrary constructions, far from scientific fundamentals.

So, an important issue for the concept of Risk is provided by Subject's attitude towards an identified Danger: passive, or active.

In the case of a passive Subject, as described in section 2, Danger, as well as Risk, are regarded objectively, scientifically, and strictly intellectually, with the most chances to use mathematics or objective estimation in their measurement. The relation between a passive Subject and Danger is descriptive, analytical, and epistemic, but also distant, without references to any action the Subject should or should not take either in connection with that Danger. This case would describe a "passive view on Risk".

If the rapport between Subject and Danger includes an action by the Subject, the relation becomes active and intensely connected to the Interest pursued by the Subject, either directly linked to the Danger or not linked at all. In this case, the *role* of the Subject brings a crucial element, the DECISION regarding an action he would take. Here, what I called Action can actually be a series of actions or a continuous long participation to a decision-making activity or Command and Control regarding measures to be taken to serve the Interest / commander's intent. These decisions and measures can be taken to counter the considered Danger or can have no relation with that Danger, or with a series of dangers. These cases describe a deontic role what can be termed an "active approach on Risk". This role is the same for both dovetailed situations described in section 2: when the Subject is active in the sense of countering the identified Danger; or when the Subject is active in general (performing a certain activity, not related to the identified danger, but susceptible to be influenced by the identified danger).

5. Threat

Another extremely important element is the character of the action considered to be a Danger, namely if this action is an impersonal event, with no intended connection with the Subject, like a hazard, or it is the hostile action made by an entity having its own will, which *intends* to cause negative effects against Subject's Interest. The hostility component is very important because it

clearly separates the Subject's reaction mode towards the Danger, and defines necessary clarifications in Subject's own structure and functionality.

This type of Risk, where a *Hostile entity* interferes, is the THREAT - the Risk perceived by the Subject who identifies a Danger as being an action prepared by an Entity which is hostile to Subject's Interest. Obviously, the term Threat limits the risk domain to the social environment (and animal kingdom), including security in military or political sense, even economy, and games. Threat does not apply in the general sense, where Risk can be generated by natural phenomena or accidents - hazards with no intended link to Subject's Interest.

Defining Threat is similar to *identifying Danger* and *defining Risk*, but much more difficult, because, while Risk is *detected* as result of observing *Risk factors*, accumulations, and developments of a dangerous nature, Threat requires, in addition, the *detection of the hostile intent*, which does not have a physical character, yet is identified with intimate mechanisms of an *entity with free will*. Among the elements of Danger, the Impact and Urgency probably become more difficult to estimate. In the same time, the Probability of incidence is somewhat simplified by scoring up, because hostility supposes energy focused to encrease the chances of completing the action defined as Danger.

An important feature of Threat, provided by the component of hostile intent invested by an entity with sovereign will is the *directional character* of Danger. This feature reflects the focused and determined pursuit of the goal to cause a negative effect upon Subject's Interest. Thus, the Risk generated by a natural Danger can be avoided, in principle, by removing the Subject from the area of impact of the Danger. As examples: the Subject takes cover from the rain and does not get wet anymore; while, on the contrary, the Threat from a hostile dog persists even after the first evasive action taken by the Subject in the attempt to avoid being bitten by the dog.

This feature influences the factors in the expression of Risk, especially in the situation when Risk is expressed by a margin of values, as follows:

- The Impact is maximized, is estimated by its maximum value. For example, the impact of a bullet is considered / feared at the maximum value of the technical killing effect, when shot by somebody determined to kill;

- The Urgency of the action with negative impact is also considered at its maximum value, because it is assumed that the hostile entity would seek to achieve surprise, precisely to obtain a maximum negative effect;

- The probability of incidence is increased, obviously, because the hostile entity employs energy, resources and intelligence in an organized manner to get things done. For example, if an angry neighbour is eager to scratch my car parked on the street, he will probably succeed;

- Even the coefficients of these parameters are increased, as well as the Relevance of the Danger, as a combined coefficient, because the Subject perceives Danger much more intensely if this is conceived and developed by a hostile entity. Different psychological resorts, functionalities, feelings, and attitudes are triggered in case of the Threat, based on Subject's past experience and profile, as introduced above.

All these considerations do not require a different expression for Threat from the one describing Risk, it is just an adapted estimation to correct the values of the Danger elements and its Relevance.

If the hostile intent is directed towards another actor, the contemplated action can still generate a negative impact upon the Subject in discussion. In this case, the Subject perceives a Risk associated to the unfavourable action, but not a Threat, because there is no directivity towards him from the Danger. For example, the Risk of being hit by a stray bullet when two other individuals or two gangs hostile to each other are fighting near by, but have no hostile intention towards the Subject in discussion.

The elements of Danger enhancement in the case of Threat also reflect the general common sense perception that Threats represent the worst category of Risks. The reason is that the other Risks have an *indirect* character, as they do

not pursue harm to the Subject's Interest on purpose, "do not take it personally". This explains why many risk management theories simply place Threat above Risk, on the "evil scale". This approach underlines the level of Danger, but ignores that the difference is given, basically, only by the hostility component. It also offers another explanation to the confusion made in considering risks and threats all together, or considering threats just worse than risks, thus making it difficult to operate practically with these basic concepts in the security domain.

Just as the Subject can be a collective subject, the hostile entity can also be a collective actor, or it can associate other entities to the hostile intent. So, the relation between Subject and Danger gets more complicated, and complex Subjects such as institutions, nations or organisations activate specialized components to deal with hostile entities.

This specific feature brings important implications to Subject's functionality, with specialisations necessary to overcome the protection measures taken by the hostile entity to keep the hostile intent secret. Such specialisation is intelligence, which seeks to detect enemy intentions, capabilities, actions.

The discrimination between Risk and Threat based on the hostility component leads to the conclusion that Risk can be high / large, such as the risk of rain during the monsoon season in South-East Asia, or the risk of a traffic accident when the brakes fail at high speed. There are, as well, lesser Threats, like the threat from a puppy who clearly expresses hostility by loudly barking at the Subject from behind the bars of a sturdy cage.

Another important issue regarding Threat is realized by the metaphoric, poetic language, where the source of Danger is personified and is bestowed with hostility, even if the source of Danger has no direct relation with or intention towards the Subject whatsoever. One can speak about "threatening clouds" or the "threat of storm". In this case, the confusion between Risk and Threat is increased by the trend to consider a Threat just a more serious Risk, because the sense of word "threat" suggests a more significant negative effect.

6. Vulnerability

An intersting situation in Risk appears when Danger is facilitated or even generated by structural or functional features of the very Subject, albeit individual or collective. These internal downfalls or gaps can lead to the increase in the assessed values of all elements of Danger (Impact, Probability of incidence, and Urgency). They also lead to an increase in Danger's Relevance, once the Subject becomes aware of such problems. Such negative structural or functional feature of the Subject, which acts as a risk factor jeopardizing the Subject's Interest, and facilitates or generates a Danger, is a VULNERABILITY.

Of course, Vulnerabilities can be exploited by the hostile entity, if known, for the conception and application of a Threat. This is why their existence becomes a secret protected by the Subject, who needs to diminish Danger, and sought by the hostile entity, who wants to increase the Danger intended against the considered Subject.

As Vulnerabilities joepardize Subject security, knowing them is important to correctly establish all elements of Danger - Impact, Probability of incidence and Urgency; but also, to realistically estimate the Relevance of Danger and thus, establish a realistic definition and evaluation of the Threat, in view of a proper Command and Control / risk management.

7. Risk management

Through the idea of actions taken by the Subject, the whole problem of the relation between Subject and Danger enters the domain of Command and Control / Risk management. Here, we talk about the Subject's activity regarding Danger, either directly to counter Risk, or in the context of protecting the success of another action by the Subject, when Danger can jeopardize Subject's action with respect to the Subject's Interest.

Writ large, one can consider that Risk management includes all activities linked to Danger, even before the Danger is *identified*, starting with *monitoring*

the Security Environment. After defining the *State of normality*, the Subject observes the *phenomena* and the *actors*, defines the *Risk factors*, i.e., the elements which can develop in an undesired way. Then, with a baseline established, the Subject can better detect *anomaly indications* associated with possible Dangers, as well as, also identify *Opportunities* of action.

However, in a strict sense, Risk management includes only the activities directly deciding the Subject's *action* meant to counter the Danger and diminish Risk. When Danger cannot be avoided, Risk management works to decide the measures to diminish the negative effect, or to delay the moment when Danger strikes. For example, when rain is forecast, we leave home with an umbrella; or, we try to live healthy aiming to delay aging.

In Command and Control, this activity can become an iterative routine of "goal seeking", where, when the planner tries to mitigate one Danger, he introduces decisions generating actions which cause new assumptions and the recalculation of probabilities. Then, the planner makes another decision, and so on.

In the same time, Risk management includes the relationship between the Subject and Dangers anticipated as possible only after certain actions by the Subject. This can be demonstrated in the logic of chess, where the players consider problems which can surface after the projection of next possible series of moves. In this case, the Subject willingly exposes himself to possible dangers, which is called *assuming a risk*, or *taking chances*. The term Risk has now a different meaning, to include important nuances introduced by Subject's active attitude towards Danger. Risk is no longer just a measure of Danger, intended to be as accurate as possible, but is now part of a complex enterprise managed by the Subject, which includes more than an estimation. Among these new ingredients of the equation there is the Subject's *Intent*, the strategy pursued to serve the Interest, and the psychological components linked to Subject personality: panic, fear, caution, prudence, dearing, courage, and bravado.

Practically, if the Risk that an action fails is estimated by a probability of 60%, the Subject can still decide to start that action, such as, for reasons pertaining to his prerogatives as a sovereign actor. This reflects the Subject's increased level of acceptable risk. A simple example is, again, participation to lottery, and thus avoid the debatable cases in military history.

Because Risk management includes decision and action, it is interesting to notice that the Risk diminishing measures can take subtle shapes, such as through measures woven strongly into the fabric of human society, in social attitudes, and moral conduct. For example: "save the women and children" - with the goal to preserve the species; hygiene - for maintaining good health; or even morale - designed to protect the spiritual interests, located on top of Maslow's pyramid. There are also extreme examples: the Holocaust - meant to protect the "pure race"; the deportation of five entire populations in the USSR (accused by the Soviets to have collaborated with the Nazis); or the isolation of ethnic Japanese in the United States after Pearl Harbour.

A special situation is Risk management in conditions of high uncertainty. There are cases when too few identification or measurement elements are available to estimate Danger, yet the Subject has a solid perception of Danger. There are also cases when the Subject perceives a large number of possible Dangers. Practically, the range spans from the simple fear of darkness to paranoia (where Dangers are detected everywhere). In these situations, defining Risks becomes a task which overwhelms the Subject's analysis capability, and Risk management is paralized.

Regarding Threat, as a special kind of Risk, controlling the situation by the Subject is not very different. Let's remember that there is no special term, there is no "*threat management*", the business is "Risk management". There are, however, functional particularities in treating threats in Risk management, by focusing on actions to counter the hostility due to human factor. We talk about a special attention to hostile entities, their intentions, and options. The difference

can be compared to the situation in the judicial domain: in justice there is prosecution regarding facts (*in rem*), when the purpetrators are not yet known - in the case of impersonal Risk; then there is prosecution regarding individuals (*in persona*), meant to establish the legal qualities of various individuals in the trial (defendant, whitness) - in the case of Threat.

An example of action levels in risk management is the difference between anti-terrorism (attitude, line of thought, campaign or demonstration), on one side, and counter-terrorism (practical action or general type of activity, organized and conducted by specialized governmental structures), on the other side.

The practical activity in Risk management means planning various *measures designed to decrease the values of Danger elements* in the view to diminish Risk (*mitigation measures*). Planning efforts aim in four directions: forces (manpower, training, new specialities, moral, and structures); capabilities (all kind of resources other than people: money, armament, equipment, buildings, and roads); regulations (laws, regulations, norms, doctrine, policies, and programs); and, measures to be requested from other structures than Subject's own (through hierarchy lines or by cooperation).

Regarding Impact, Risk management covers both the initial impact of the undesired action, and the later effects thereof, the aftermath, by activities of *damage control*. The planning measures in this respect target the *risk factors* that generate or enable the Danger: the *cause* and *enablers.* Mitigation measures regarding Impact cover a large variety of possibilities: for example, they may aim even to adjustments in forces' perception on Interest, such as development of values like patriotism and commitment for balancing the fundamental preservation instinct vs. Danger.

Regarding the probability of incidence, the mitigation measures aim at risk factors identified to increase the chances of Danger coming true. This requires more imagination and out-of-the-box thinking, which underlines the value of creativity and imagination in analysis and planning. Mitigation

measures regarding the probability of incidence start from *security environment conditions*. Considering Threat, these measures go as far as the actions meant to decrease even the basic threat factor, that is the hostile intent. These are the *deterrence measures*.

Regarding the Urgency, specifically the *moment of incidence*, the mitigation measures are meant, of course, to *delay*, as much as possible, the moment when the undesired action occurs, or to delay the pace of aftermath effects. All risk factors influencing the *Danger timeline* are considered in this respect.

8. Knowledge development and intelligence

Although the *effects based approach* (EBA) has been discarded from current operations (some would say for good reasons), its value remains in planning and long term risk management in general. Even so, logically, EBA cannot be ruled out from planning future operations and *Future Security Environment*.

It is consistently true for *knowledge development*, which provides the informational basis for risk management analysis by *understanding* the Security Environment and *illuminating* the *causalities* and the *courses of action*. Knowledge development should include the definition of the *state of normality*, in strong connection with Subject's Interest, and described in documents with legal, political, or operational value. The definition of the state of normality is necessary before monitoring the risk factors and identifying indications of anomaly, and thus helps setting the *level of ambition* / the goal and the *end state* for the mitigation measures. For example, the state of mormality in security is obviously different in Switzerland from that in Iraq or Somalia.

In the case of Threats, intelligence is crucial to support risk management by detecting and documenting the hostile intention and enemy planning. Intelligence is crucial for risk management also because of its value in warning, which provides greater chances of success in planning and applying mitigation measures. If warning comes soon enough, by rapid identification of possible

Dangers and providing actionable intelligence in prognoses and evaluations, risk management is able to provide mitigation measures in time to obtain the desired effect of preventing the Danger or limit its effects. This would be what is called "early warning" and its value explains the amount of resources allocated to intelligence in the whole Risk management architecture of the Subject's organisation (For example, the size of J2 in an operational headquarters).

It is probably worth pointing out here the different meaning of Risk in intelligence and planning, and within Risk management in general, given by the different roles of compartments. With a scientific and intended objective approach to Danger, intelligence is the epistemic authority inside the Subject, and has a passive attitude towards Risk. On the contrary, Risk management plans the Subject's actions to counter Danger, and establishes the Risk that the Subject is confortable to take or accept in pursuing its Interest. Since the Risk management / Command and Control is about decisions and actions, it represents the deontic authority in the Subject architecture and has an active attitude towards the Risk, it views Risk with a different meaning compared to intelligence, which represents an epistemic authority.

Conclusions

Instead of starting from complex risks and threats which cause great concerns in the present international environment, the thoughts presented here have approached the fundamental elements of risk theory through the basic bricks of the generalized situation picturing an individual coping with the problems of the Security Environment. Looking at the simplest elements, the individual, called the Subject, sees good and evil around, evil firstly, and tries to do something about it. This situation includes an actor - the Subject - and an action with negative perspective - the Danger - within the Security Environment. The author has argued that the relation between Subject and Danger describes the issue of interest - the Risk, albeit in the worst form - the Threat.

Dwelling on the basics, the author found merit in examining Subject's role in this relation and in breaking down the structure of Danger, to its own building bricks and either its natural or hostile cause. Here, the nature of Threat is probably more useful to be considered in its hostile component than simply as a worse Risk. The author thinks that the elements of danger and their coefficients of importance, reunited into the combined coefficient here termed Relevance, are useful to organize analysis and planning. Thus, the values of Impact, Probability of incidence, Urgency, and Relevance can be practically used in structuring the risk management activity.

The author thinks that the difference in Risk seen by intelligence, and Risk seen by planners is a fact of life in the security domain and should not be fought, but understood and accepted by risk management scholars and practitioners.

This paper also points to the level of expectations towards the possibility to use mathematics in risk management, where the analyst always sets the balance according to his honest views, while producing assessments; and, the decision-maker is free to lead actions according to his sovereign will and the views of the best way to serve the organisation's Interest.

Follow-on papers in this domain should probably treat the mechanics of analysing the risk factors and further common concepts for all domains performing risk management, as well as, further develop possible additional math and logic expressions of the parameters presented and discussed within this paper.