FOCUSING AUTOMATED DECISION-MAKING

Edouard Valensi
French Minister of Defense
DGA – DCI
00460 ARMEES
France
Tel 33 1 45 52 43 95
Fax 33 1 45 52 49 86

It is without doubt in complex logic applications and especially in the fields of command assistance, that information technology has encountered the greatest number of obstacles. Military leaders have been expecting results “just around the corner” for more than 30 years now, but time has passed with no decisive outcome.

Progress has of course been made

- In the automation field where real-time shape recognition enables routine automatic target acquisition and homing. However this is no more than an elementary, animal type of intelligence that falls short of the taking of complex decisions,
- Procedures allowing the automatic generation of repetitive commands (for organizational optimization for example), but the decision-making rules employed are pre-ordained, with no consideration of the unexpected situations, here lies significant hazards.
- Sometime, neural networks enable experience and learning substitute for formal analysis, but this is only possible in foreseeable situations and once more the unexpected stays scarcely controllable.

This limit has to be identified and it must be accepted that automated decision-making have to be considered as an extremely hard discipline. To accept this reality in the military field implies:

- restricting our ambitions to expand through continuity effective capacities of decision-making aids from mastered domains,
- Steering away from any too-direct transposition of ordinary decision-making procedures.

Studying decision-making in the tactical field help to identify stumbling blocks that have to be overcome and drawn possible areas for research.

1. An analysis of an air-naval strike.

Thus to formalize a decision-making process, an elementary tactical action (the archetype of which is to fire a missile against a hostile that appears to be making a surprise attack on a ship) that can be taken as an example. Awareness of this threat gives rise to a situation out of which an irreversible decision must be taken, whatever happens; fire the missile or risk seeing the friendly site, that one should have protected, hit.

Automating decision making is only of advantage if it can be taken safely, before the authority that would have had to decide to fire would secure access to full information. If the information is available, in other words a "natural" decision is possible, it is neither necessary nor desirable to resort to an automated procedure, which retains an element of chance. Therefore, automated decision-making is not justified under normal circumstances, but in crisis situations where decisions must be taken in a rush, with incomplete information. The risk generated by this lack of information has to be minimized.

When is the decision occurring? It is taken at the precise moment when the weapon is fired; the instant that the trigger is pulled, what follows is just automatism. As for the decision itself, whatever its nature, it aims to maximize a function (or minimize a cost) within a set of constraints. To establish this cost function we need a descriptive language for the situations encountered, bring down to its skeletal form, it reduce to the following elements:

If the weapon is fired, three situations may arise,

- T1: destruction of an attacking missile or aircraft (good decision),
- T2: fire against a non-attacking object (risk of friendly fire or worse, destruction of a civil aircraft),
- T3: weapon firing against a non target (false alarm)

If weapon firing is refused, two situations may arise:

- R1: the ship is destroyed (wrong decision)
- R2: the threat disappears spontaneously.

A range of probabilities and costs are associated with these eventualities:

- p_1 false alarm probability (firing against a non target), cost: c_1
- p_2 probability of error (destruction of a civilian aircraft) if a threat is identified, cost: c_2
- p_3 probability of correct identification of a threat, cost: c_3

$$p_1 + p_2 + p_3 = 1$$

- q_1 probability of error in the case of non-identification, cost: d_1
- q_2 probability of correct identification of the absence of threat, cost: d_2.

$$q_1 + q_2 = 1$$

c_2 and d_1, which represent the cost of incorrect identification, have a very high value, as collateral effects can be particularly counterproductive and, conversely losses weigh heavily on the balance sheet; c_3 corresponds to the cost of an interception missile; $d_2 = 0$, as no missile is fired and no damage occurs to anything.

Initiating the engagement of a presumed hostile result primarily from arbitration between the costs of the two types of error: $p_{2}.c_{2}$, - collateral damage - and $q_{1}.d_{1}$ - loss of own unit - which it would have been possible to prevent. This arbitration occurs after sight of an event assessed as significant, generating an alert and after taking account of:

- The risk, which includes an appreciation of the friendly force situation,
- An estimation of the location and intentions of an adversary,
- An appreciation of the costs associated with each of the possible errors.

2. Decision parameter are highly dependent on the military and political context.

When evaluating these probabilities and costs it appears that the values are highly dependent on the associated military and political context. The nature of the military operation is consequently an essential parameter to be taken into account. Relatively to military operations, figure (1), a typology of military situations,
represents both a reference and a basis for analysis.

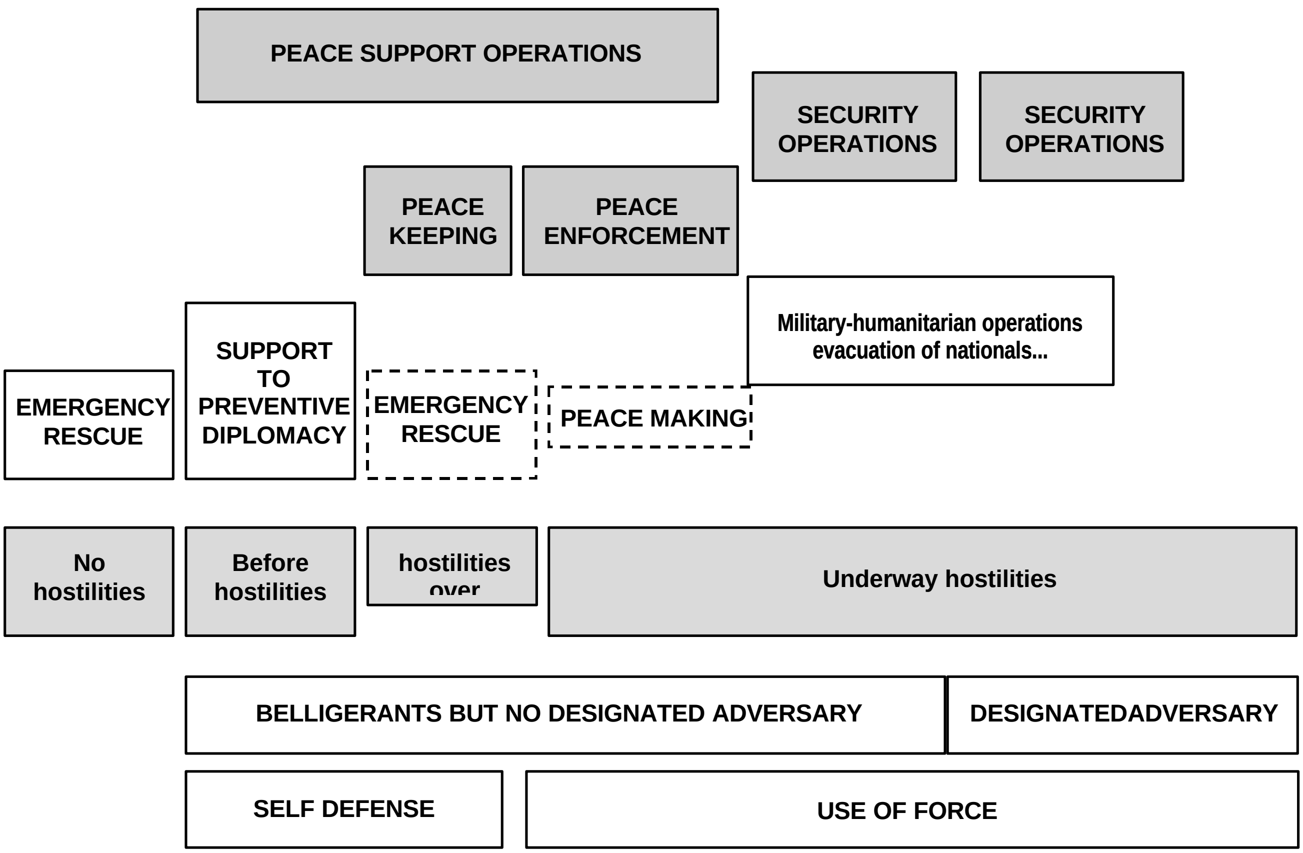

Figure (1) A Typology Of Military Situations

Briefly, these are the main statements:

- Limitations of a political nature and the appreciation of collateral damage will be all the higher the further one is from a state of war,

- In an international policing environment, units in contact may be provoked, and (returning to the example of an attack on a ship) friendly warships may find themselves confronted with feint attacks creating an atmosphere of tension, and hence a source of error,

- In a peace time situation where the probability of attack is low, the probability that detection of a threat might originate from a malfunction of the warning system, or from an error in the position of friendly forces (source of incorrect interpretation), may be higher than the probability of a genuine attack; $p_2 > 0.5$. This probability would be completely different in the case of open conflict.

Whatever the nature of operations, the military situation contains elements of uncertainty and the hypotheses that are associated with these, the “pre-assumptions”, must be identified. Pre-assumptions may concern opposing elements, enemy forces or weather conditions. For them to be explicitly mentioned, they must be:

- Necessary, in other words influence an important factor or fact that is essential to the appreciation of the situation (here the assessment of probabilities),
- Plausible, in other words coherent with the current or future situation,
- And above all verifiable. Verification process has to be completed before the operational decision is taken (hence the advantage of delaying irreversible decisions as late as possible).

Outside war situations, when assumptions are stated, amongst the parameters that should be considered, the following must be remembered

- False appreciation of friendly situations (position, condition of forces, etc.), false appreciation of the threat (incorrect assessment of a very low probability),
- Irrationality of an adversary.

3. Minimizing the risk of error

Let us now turn to automatic weapon engagement procedures. In the context of uncertainty where decision assistance assumes all it value, the foremost purpose of automated decision is to minimize the risk or error.

To reduce this risk

1. The decision-making process is broken down into three phases:

a) Appreciation of the political risk and military environment, which determines a form of behavior (is one in an alert situation, crisis or war?) and sets the decision-making procedures,

b) The decision itself, which must remain qualitative in nature: (fire or hold decision),

c) Optimization of decision making conditions, (with the optimum assignment of means, optimization of trajectories, observation of the results).

2. Irreversible actions are committed as late as possible: this can be achieved:

a) By breaking down the decision-making process into

- A decision preparatory phase (reversible),
- The irreversible decision commitment phase (programmed as late as possible),

b) By authorizing changes by commanders at any time to decision-making procedures (new appreciation of the political risk and the military threat environment) and especially by making provision for an instruction to cancel firing of a weapon already engaged.

All the previous considerations are included in a generic functional organization chart figure (2), bringing out the relations that develop between.

1. The module that assesses the political and military context that will determine the parameters for the three decision-making functions: weapons ready, weapon release and any termination of engagement or the possible destruction in flight of an interceptor missile. (Alert is sounded automatically once the sensors, regardless of the context detect a threat).

2. Optimization of the engagement process breaks down into two phases: preparation for firing and the decision to fire itself, which is delayed as long as possible. (Here there is undoubtedly a significant difference between a war situation where, to avoid the risk of saturation one tends to open fire as soon as possible, and situations in peacetime or involving the international maintenance of order).

3. A security principle that must leave the commander the option of interrupting the engagement up to the last minute.

Note that, even if automated, conditions for firing weapons are not changed in their fundamentals: qualitative decisions are still a command responsibility (even if they are taken after the weapons firing itself or are coded into the decision-making algorithms), the man must be able to follow the engagement process and qualified authorities can interrupt it at any time; weapon systems and procedures will gain from being designed with this in mind.

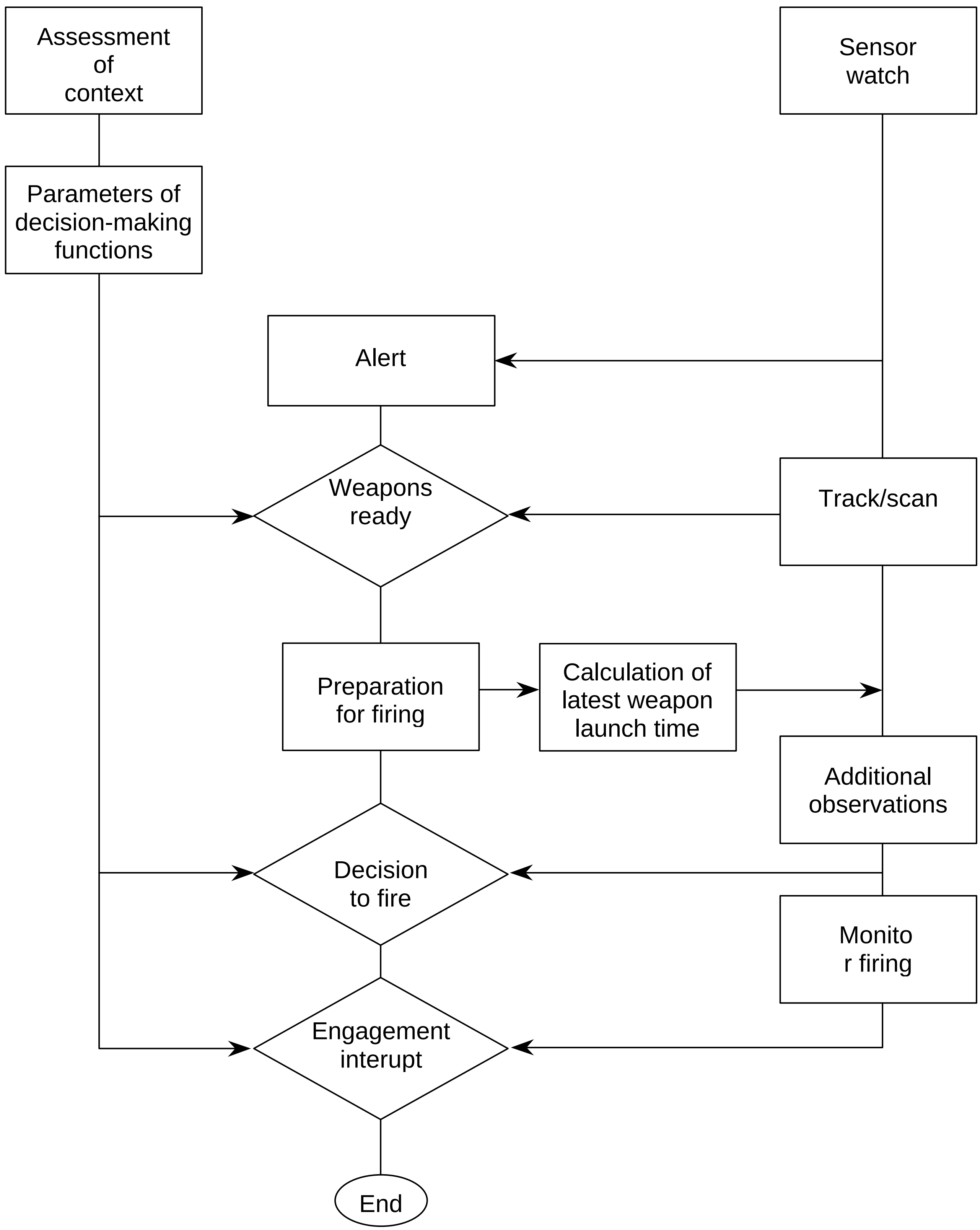

Figure (2) A Generic Functional Organization Minimizing Risk

4. To move towards more complex decisions.

Can one go further and deal with decisions involving whole units, getting close to operative level? This is what everyone wants. However, as a result of the issues outlined above, the following aspects must not be forgotten:

1. In the example of a missile firing, decision-making assistance is first a procedure to minimize risk, and not only a simple translation of human behavior. A specific ultimate aim justifies and broadens the transposition of operational duties. It should be sought in every case.

2. The system distinguishes clearly between the stages where decisions are taken (they are qualitative, few in number and decisions are of a binary type) and the optimization phases located downstream which bear the consequences.

3. To set out relevant decision-making algorithm, we must first rely on a complete and precise language enabling operative situations to be described in all their complexity.

4. Validation modules for the assumptions are essential (they would precede the final fire decision and any decision to interrupt the engagement). To dispel uncertainty, a fusion of signals from independent sources may be determinant. In this way a "Top down" approach to battlespace awareness is a result of the "Joint force automated battle rules of engagement".

It is probably necessary to move towards a mastery of the cybernetic analysis of operative decisions before undertaking a major conversion to automation. But the sequence of logical action will certainly take different forms depending on the nature of the decision that has to be automated (collaborative planning have different constraints than Automated rules of engagement or Automated support of simultaneous, coordinated operations), and so a significant number of specific cases and military situations will need to be studied before any general rules could emerged for automating aids to the command function.

For the moment we should surely develop an operative level descriptive language; surely we should have decision flow charts, to the same scale as databases describing real situations? If we take account not only of the weaknesses of IT (rigidity, lack of imagination, lack of reliability when faced with unexpected situations), but also its strong points (infallible memory, rapidity of identification of a reference situation) we can seek to collect the maximum number of example engagements, false alarms, risk identification, etc.

As the Director of Defense Research and engineering stated in the Joint Warfighting Science and technology Plan: *At this operative level that the lessons learned from exercise, and even more so the post mortem analyses of real operations will be most rewarding. It is at this level, where a highly developed imagination is required, that a comparison of approaches, made possible by international cooperation, might be particularly welcome.*