introduction of the continuing inventions of increasingly sophisticated information technologies into command, coordination, control, communication and intelligence systems (C4I) forms a fantastic blessing for the quality and effectiveness of future operations (cf. Toffler & Toffler, 1994). However, it can be seriously questioned whether such optimism is really justified. Isn't it often so that promising innovations are often too good to be true? Isn't it often so that every promising development contains at least some *dis*advantages? Isn't it often essential to ask more specific questions with regard to potential effects of innovations such as: in what respects will it have an impact and to what extent do the advantages outweigh the disadvantages?

In order to come to a deeper and more balanced insight, this article will focus on one specific area of warfare, namely the area of (early) warning responses and military and political preparedness against impending dangers. It will be concentrated in particularly on the question: Whether, and if so in what respect the application of modern information technologies and forms of information warfare will have positive and/or negative implications for the state of preparedness of military commanders and political leaders during encounters with actual or future dangers?

The outline of this article will be as follows. First, I will elaborate briefly on the essence of political-military preparedness and warnings. Then I will subsequently discuss the impact of new information technologies and information warfare on several factors that tend to be crucial in explaining serious shortcomings in the so-called intelligence cycle: i.e., the detection of potential dangers, the collection of signals and threatening patterns, and interpretation and dissemination activities (cf. Kam, 1988; Levite, 1987; Wirtz, 1991: 4-13; Handel, 1987; Metselaar, forthcoming). After that, I will briefly focus on the likely impact of "new" information technologies on the awareness, acceptance, coping responses and defensive preparations and preparedness of political and military leaders (see also Figure 1). The article will be closed with a few tentative conclusions and recommendations for further research.

Figure 1: Conceptual model of the presented analysis

POLITICAL-MILITARY (UN-) PREPAREDNESS AND WARNINGS

Preparedness can be characterized as a familiar, but at the same time complex and multi-interpretable and normative concept. In order to understand the implications that the ongoing introduction of modern information technologies may have in the nearby future, it is therefor necessary to start with a definition of preparedness. The following definition combines elements that according to descriptions in dictionaries, military doctrines, war studies and procedures can be regarded as essential for preparedness (cf. Metselaar, forthcoming):

> The degree and appropriateness wherein an actor (in this article specified as a small selection of individual political and military authorities in key positions) is mentally, conceptually, physically, organizationally and politically ready to respond as optimally as possible (given his potential capabilities) to (various aspects of) a danger during the first phases of an actual encounter.

Preparedness can be distinguished into three closely interrelated dimensions:

1. *The first dimension is formed by the state and appropriateness of the mental anticipation and alertness (of key decision-makers) with regard to the actual materialization of the (predicted) danger as well as its immediate effects and its probable immediate and long-term implications.*

This dimension refers to the degree wherein key military and political authorities mentally and conceptually anticipated on the actual confrontation with the striking danger. More specifically, this dimension encompasses the degree wherein the direct responsible political authorities *mentally* anticipated and were in a moderate to high state of alert with regard to (a) the probability of an offensive; (b) the type of action(s) that the danger unfolds; (c) the location(s) on which the danger (the adversary's offensive) was directed; (d) the timing of the confrontation; (e) the strengths and weaknesses of the danger (i.e., the enemies troops against versus the strengths and the weaknesses of the defense (capabilities, organization, but also mentally); (f) (in case of a danger in the form of an attack) the objectives of the offensive and its place in the enemy's strategy; and (g) its (immediate) impact and consequences.

2. A second essential dimension is formed by the state and appropriateness of a decision-maker's awareness, and readiness to make use of conceptual, physical and mental components of the "basic measures" and "emergency measures" that can be applied almost immediately when a danger strikes in order to minimize the immediate and long-term risks and costs of the impact of the danger.[1]

3. *A third dimension of preparedness that can be crucial for policy-makers (in particular during operations other than war) concerns the degree wherein national authorities have build up sufficient political acceptability and support that can be needed to ensure sufficient (political and public) acceptance and support as far as this is required to respond as optimally as possible to the danger and its effects.*

This dimension refers to the decision-maker's state of anticipatory protective counter-measures and attempts of "public educating" to ensure the political acceptability and consensus that might be needed (a) to cope with (i.e., prevent or minimize) the impact

> and/or the implications of a encounter with the impending danger itself; and (b) to ensure the political and public acceptance and support that might be needed to ensure the feasibility and effectiveness of rapid counter-measures as well as support for the possible implications of these counter-measures. This may include the support or at least the acceptance from groups/actors who are not directly involved with the military operational aspects (e.g. the press, the public, other departments, potential allies) adequately anticipated the confrontation with the danger and its consequences and were ready to cope with it and (in case of a democracy) were ready to support possible crisis management options of their government (Cf. Handel, 1982, in: Gooch & Perlmutter, 1982: 149).

"Warnings" can be regarded as container term or a *label* for …

> A combination of indicators, patterns, as well as oral or written messages that may be observed, heard, read, or reconstructed by one or more receivers (i.e. the selected key authorities and/or parts of their organizations) whereby this data provides more or less ambiguous, uncertain, detailed and reliable predictions about (one or more dimensions of) a potential danger, and whereby this data may at least potentially create a sufficient time span to prepare protective counter measures (cf. Metselaar, forthcoming; Levite, 1987: 174; Kam, 1988: 24, 29).[2]

Just like preparedness, warnings consists of various dimensions. The following dimensions can be observed in most intelligence cycles and warning processes: (1) Content; (2) warning span; (3) accessibility; (4) reliability; (5) quality; and (6) quantity. Laboratory studies and studies on organizational and public communication have indicated that these dimensions, and more in particular the combination of specific values that are taken on each of these dimensions can significantly affect the leader's sense of awareness, and willingness to accept and respond to warning signals.

After defining preparedness and warnings, it is now time to elaborate on the likely impact that the application of the wealth of "new" information technologies that have been referred to in the opening of this article, may have on (1) the process of detection of potential dangers; (2) the collection, dissemination and interpretation of potential warning signals; (3) the awareness, interpretation, acceptance, coping responses of military and political leaders; and (4) their state of preparedness during encounters with actual and future dangers.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON *THE DETECTION AND COLLECTION* OF THREAT INDICATORS

For intelligence agencies like the National Security Agency and the Central Intelligence Agency the impact of new information technologies on the collection of potential warning signals and threat indicators with regard to a wide range of potential dangers is still increasing. Early warning systems, possibilities for interceptions and eavesdropping, as well as technological possibilities to collect visual and transcribed facts and figures about actual developments on potential battle fields are becoming more widespread and sophisticated everyday. In turn, this will usually makes it much easier to exchange important intelligence from intelligence agencies of other countries. It will make intelligence agencies with less sophisticated capacities and expertise more dependable in times wherein they are confronted with impending dangers. At the same time, experiences like the Gulf crisis and the Gulf war, Pakistan's unexpected tests of nuclear devices during a crisis with India in May 1998, the Kosovo air campaign and several unexpected moves from Milosevic and his army, have once more underlined that one must be careful not to over-estimate the power of technologies. Many static and more in particularly *mobile* objects are still difficult to trace with certainty, especially when they have to be identified from great heights, in short time, and under poor weather conditions. Dummies can still be used remarkably successfully in order to create serious misperceptions and threat estimations.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON *THE DISSEMINATION* OF (POTENTIAL) WARNING SIGNALS AND THREAT ASSESSMENTS

The last decade, and in particular the last years as well as the nearby future suggests that (in comparison with the possibilities to collect warnings) the biggest innovation in the field of "preparedness and surprise attacks" appears to be made in the field of dissemination of intelligence, C4I-aspects and the decision cycles (Leonard, 1998). In principle, potential attackers as defenders may profit in many ways from this. At the same time it would be stupid to neglect several possible negative influences: For instance, the increasing need for real-time data may increase the commander's situational awareness. At the same time, however, it may increase the chance that the motivation of intelligence analysts and experts to double-check, analyze and interpret data as thoroughly as possible declines.[3] More than ever before analysts and staff members will have to cope with the dilemma whether they should disseminate data and advise their superiors and other allies more rapidly if they want to have some influence by policy makers and if they want to be a serious source besides a commander's other sources for information with the risk of being overhasty and losing credibility, prestige and self-esteem for wrong assessments or if they should not act in line with the increasing time pressures and creating thorough assessments that are hardly utilized. [4]

THE IMPACT OF TECHNOLOGICAL INVENTIONS ON *INTERPRETATIONS* OF COLLECTED SIGNALS AND OBSERVED PATTERNS

Past as well as recent experience reveal that the introduction of new information technologies tends to have a profound impact on most dimensions of the warning signals. It is quite likely that this impact will be even more impressive and in many senses still impossible to oversee in the recent future. Let us look more closely at the likely impact on several of the warning dimensions:

Dimension 1: "Content"

Warnings may encompass pieces of information with regard to one or more of the following content aspects of an impending danger: [5]

(1) An estimation of the probability that the danger (the attack) will materialize (*whether*);
(2) Identification of the precise identities of the attacker(s) (*whom*);
(3) A determination of the type of actions and technologies involved (*how*);

(4) An identification of the location(s) that will be in danger (e.g., that will be attacked) (*where*);

(5) A prediction of the timing when the danger may be materialize (e.g. the timing of the attack) (*when*), and.

(6) An assessment of the reasons and objectives (motivations, causes) behind the danger (*why*).

At first sight it seems obvious that the introduction of modern information technologies will make it less difficult than ever to improve the quality of warnings on each of these content aspects. Although, it will still be necessary to guess a lot and to rely on a combination of luck, *Fingerspitzengefuhl*, specific experience, defenders will be confronted much faster, with more detailed, more reliable and better controllable signals, patterns and threat assessments than ever before in the history of warfare.

At the same time, however, many biases, traps and disadvantages will be introduced as well. One relatively new structural trap that may be more relevant than ever can be called the *"What you see is what you get" (WYSIWYG) syndrome*. Leaders as well as analysts who become confronted with current, often visualized, real-time data which may potentially tell something about one or more of the seven dimensions above, will regularly have great difficulties to remain cautious for the possibility that they may deceive themselves and/or that they may be deceived by adversaries and often ambiguous circumstances. The usual strong and dominant impact of visual information on the human's mind can easily lead to profound misperceptions and failures. For instance, since it usually concerned coping with so called cynical dangers; there is always a chance that attacker changes his mind while the defender is still thinking and acting in accordance with the latest pictures that have caught his mind.

Furthermore, the actual situation of impending danger may have significantly changed because of situational dynamics and the timespan between the sending and the receiving of the signals. Although leaders may be well aware of this, simultaneously, they may frequently experience more inner pressures than ever to jump to quick decisions and actions. The fact that these leaders may be well aware that others in their direct environment see the same "real time" pictures and may began to wonder why there are still no decisions taken (they may suffer from the same syndrome too!) can become a major source of time pressure. Furthermore, doctrines and training that dictate that it can be crucial to walk quicker to decision cycles than your adversaries, as well as the impact of the press (i.e., all sorts of CNN and Internet effects) can become major sources of self-imposed deadlines as well.

Technological developments may also increase the chances that leaders and analysts fall into another cognitive and psychological trap as well. That is, people may become more or less obsessed by the visual, real-time data they become confronted with, spending most of their bounded time and span of attention to it. The price may be that they almost completely overlook crucial, but (at least for them) perhaps less accessible and controllable, and more complex *background* intelligence that could have told them more about one or more of the content aspects of the impending danger.

Dimension 2: The ”warning span dimension”

Another crucial dimension of warnings is the so-called *time span ratio* between the moment of warning issuance and the moment whereupon it is predicted that the warning may probably materialize (when nothing is done). This dimension is often described as the “warning span” or “warning interval” (Kam, 1988: 22-24, 29, 32-33, 57-59; Chan, 1979: 171). Ideally speaking (from the perspective of a defender) detailed and reliable warnings are issued at a moment upon which they still have sufficient time to prepare adequate counter-measures (at times including the option of a pre-emptive strike).

Historical evidence reveals that the introduction of various technologies during the past centuries has had an enormous impact of the warning span dimension. Probably the greatest revolutionary change in warfare and crisis management was the exponential increase in mobility. This development compressed time and space, quickened the movement of troops, offensive and defensive capabilities and supplies. As mobility increased, the warning span for counter-measures significantly decreased: From months or weeks in the early nineteenth century, to weeks and even days in the railway and combustion engine and tank period, to days and hours in the age of air power, and since the last decades to hours and even minutes in the nuclear age (see Figure 2).

*Figure 2**:** Conceptual model about the reduction of warning time due to the invention and introduction of technologies and its impact on chances to achieve surprise (derived from Michael Handel, 1989: 66).*

The trend that has been set during the past might be continued in an almost dramatic way. That is, the use of the latest information technologies by one or more adversaries may bring back the warning span to almost zero. Since information attacks and PSYOPS may be silent and hidden, it will become more complicated and sometimes even impossible to pinpoint the commencement of an offensive information attack at all, or to determine adequately who delivered it, when, where, why and how it started. It may even become unclear for some time how long threat assessments, decision-making and the implementation of counter-measures can wait before a defender’s entire C4I infrastructure is seriously damaged (at least for the time being) and an adequate response in no longer possible. In other words, the growing role of information warfare is rapidly lowering the classic barrier between war and peace. In other words, the recent technological developments may blur a defender's assessments and awareness regarding the probability, the timing, the location, the initiator and the impact of an attack as well as the attacker's strategy and tactics. It is highly likely that there may become a trend towards constant low-intensity and diffuse information warfare (cf. Thomas in: Pfaltzgraff & Shultz, 1997). In fact, forms of largely unnoticed arms races and silent computer attacks, with far-reaching forms of anticipating on (new) possibilities of a wide variety (of often unknown) computer attackers and ones own vulnerabilities are going on for some years now. They will certainly continue to do so in the future.

Dimension 3: "Accessibility"

One of the biggest structural problems with warnings that has become evident many times during surprise attacks as well as confrontations with striking disasters is usually *not* the fact that there was no adequate intelligence available in time. Instead, the biggest problem is that key commanders and authorities were frequently inadequately informed by their subordinates or colleagues about the intelligence that has been collected or produced somewhere in their departments.

Lack of accessibility can be caused by many factors. For instance, compartmentalization or too much secrecy, bureau politics, too much specialization and fragmentation (Wilensky, 1967; Wohlstetter, 1962; Levite, 1987; Kam, 1988); as well as reactions on cry wolf syndromes, fear of losing credibility in case it appears to be a false alarm, intelligence-to-please syndromes, too long and complex lines and procedures; etceteras.

It remains to be seen whether the benefits of the introduction of new technologies will outweigh its disadvantages. Indeed, at least potentially, political and military leaders will have much more opportunities to become directly exposed to intelligence and to bypass a lot of hierarchic ladders in the C4I lines. At the same time, this may easily lead to too much noise, more appetite for the wrong kind of data, information overload, a shift towards micro-management and a false sense of control. Moreover, it may lead to wrong responses in case of all the confrontations with high numbers of rough information of which many subtle details and ambiguities are simply overlooked or misperceived. Last but not least, it may structurally distract the attention and information search of leaders (and partly as a consequence of that significant parts of their organizations) away from potential signals and indicators that tend to be much less accessible, but that can be at least just as crucial for making adequate decisions and preparations (e.g., data with regard to the adversaries motivations, hidden agendas and strategies).

Dimension 4: "Reliability"

Much of the research on warning responses and preparedness indicates that the attributed reliability of sources from which a person receives signals and warnings have a significant influence on the consideration whether or not warnings should be acted upon. The higher the credibility of a source and/or a message in the eyes of a receiver, the more likely the information that is offered will be noticed and accepted without a quite critical evaluation and the more likely that people will be willing to change their opinions and course of actions in accordance with its contents. Conversely, if a source is considered untrustworthy or uninformed, incoming information is more likely to be avoided or denied. This, in reality quite difficult distinction seems to become more blurred than ever due to the impact of Internet (and CNN) as one of the most dominant and accessible sources of the latest data. It is a fascinating paradox that intelligence agencies who frequently try to affect others by manipulating information that is disseminated through Internet and news agencies like CNN can become a victim of the same media themselves. The conviction that they are quite capable to see the difference between reliable and unreliable data will frequently become a dangerous trap. A trap that can affect the quality of the whole further intelligence process as well as the degree of credibility that policy makers attribute to their agencies.

Dimension 5: "Quality"

One of the most crucial dimensions of warnings is its quality. In other words, the degree wherein a warning provides certain, accurate, timely and detailed predictions with minimal ambiguity and maximal certainty (cf. Kam, 1988: 28). Again, it is important to notice that most decision-makers will consciously or unconsciously have to make some evaluation of which warnings they appraise as accurate and reliable in a veil of ignorance about the future versus post hoc or hindsight evaluations of which warnings have been more or less accurate and can therefor be seen as high quality assessments (cf. Wohlstetter, 1962; Handel, 1976; Kam, 1988: 39-42, 50-51, 56).

Dimension 6: "Quantity"

The quantity of incoming warnings (in other words the amount of potential warning signals intelligence agencies or specific policy makers become aware of within certain time frames in comparison with there limited capacities to process them adequately) is one of the most mentioned dimensions of warnings (Wohlstetter, 1962; Breznitz, 1984; Levite, 1987; Kam, 1988: 49, 53-55). Like the other dimensions, the way quantity is experienced can be quite variable depending on what cues, signals, messages, or patterns are experienced or labeled as warnings.

For various reasons (depending on the strength and the imminence of the danger), more or less recent experiences like the Rwanda genocide in 1994, the Iraq attack on Kuwait in 1990, or the Kosovo crisis in 1998-1999; indicate that it is quite likely that the quantity of potential threat indicators that may be collected will drastically increase in number. Moreover, the same occasions illustrated that the impetus of relatively sophisticated technologies (satellites, interception capabilities) (accompanied by the widespread illusion that just the possession of better and more rapid data collection capabilities forms a guarantee for success) regularly tends to a significant increase in the organizational and decision-maker's appetite for more, real-time data. Simultaneously, however, the chance that intelligence analysts, military commanders and policy makers will regularly suffer from various forms of data overload will increase further as well. Better facilities will often create an increasing need by commanders and authorities for current, detailed, and rapid intelligence in order to increase their situational awareness. At the same time and at first sight perhaps paradoxically, it is quite likely that they will *experience* periods wherein they are significantly victimized by (timely) data *under*load. In many ways, one can observe a behavior pattern that can be seen in many other fields of economy as well. The more welfare, the higher the expectations and the more likely ambitions will be set higher and the more frustrations if needs cannot be fulfilled in time.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON FACTORS THAT FRUSTRATE THE INTERPRETATIONS OF COLLECTED INTELLIGENCE (LIKE FALSE ALERTS AND NOISE)

Four decades of studies on surprise attacks reveal that most adequate warnings suffer from an overload of distorting signals, as well as uncertainty and ambiguity with regard to all dimensions of warnings and impending dangers (Wohlstetter, 1962; 1965: 691; Handel, 1977: 462-464; 1984: 236-237; Kam, 1988: 50-51, 56; Vertzberger, 1989; Whaley, 1973). However, one of the most influential factors beyond intelligence failures and surprise attacks forms the *called Cry Wolf syndrome* (Breznitz, 1984). The more warnings and alerts that for various reasons are attributed as false (for instance, because a potential attacker has changed his mind, or because intelligence agencies were insufficiently informed about the exact time, location of a dangerous encounter, the more likely the credibility of later warnings will decline and desensitization processes will become dominant. Usually, it will lead to wrong interpretations and responses to new relevant warnings. For example, there was an overwhelming number of warnings of an impending North Korean attack before North Korea actually attacked South Korea in June 1950 thereby completely stunning U.S. and UN authorities (Doyle, in Knorr & Morgan, 1984: 80-82). General MacArthur's intelligence staff in the Far East Command which was the major source of military intelligence on Korea warned Washington between June 1949 and June 1950 no less than *1,200 times* about the risks of a North Korean attack. In one sense all these warnings were accurate because North and South Korea were engaged in a protracted artillery battle accompanied by regular border crossings of military units. The warnings amounted therefor soon to continued cries of "Wolf! Wolf!" in the eyes of most of the key political authorities in Washington. It was therefor no coincidence that secretary of Defense Louis Johnson, first reaction on the news of the invasion was to dismiss it as just another border violation.

It can be expected that the introduction of new information technology will not only contribute to the quality of warning processing and responses. It is quite likely that they will lead to various forms of sometimes devastating productions of largely irrelevant information (noise) and cry wolf syndromes as well.

Deception as another source of noise production

Deception has always been a crucial element of warfare. It is usually meant to secure concealments of someone's real intentions, capabilities, the maneuver and concentration of troops for the purpose of achieving a surprise attack or a surprising defensive move. Deception may be conducted in various forms. For instance,

- By spreading up false rumors;
- By masking the operations of radios, by setting up dummy radio nets and by radio deception;
- By the introduction of false information into security systems, data networks of state institutions and Internet.
- By setting up dummy objects and by feats;
- By concealing real objects and movements from reconnaissance and observation;
- By changing the external appearance of objects and movements;

- By artificial noises;
- By the use of computer viruses (e.g. the “Trojan Horse virus”, the “Forced quarantine virus”, the “Overload virus”, the “Sensor virus”, the “Stealth virus”, and electronic warfare.
- By sound discipline and coordination.

As recent wars and battles have shown, information technologies are likely to play a more significant role in each of these forms of deception. Deceptive information operations can cause defenders (as well as potential attackers) to make incorrect judgments and decisions. Due to the introduction of new information technologies in deceptive actions, it may become less difficult than ever to reinforce pre-existing assumptions and values about the features that a dangerous encounter will have. That is, it will be easier for a well-sophisticated aggressor to feed a defender’s expectations in various well-coordinated ways with a number of subtle at first sight highly reliable hints. It may also become easier to enter the decision-making cycles of adversaries via information technologies. Moreover, due to strong innovations in the interception systems, it may become easier (that is at least in technological respect) to double-check whether and if so, to what extent, an attacker’s as well as a defender’s deception strategies and tactics are successful as well.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON *THE CAPABILIES TO UNDERSTAND, INTERPRET AND RESPOND TO* COLLECTED WARNINGS

At least since the last three decades, studies in Communication Science, Cognitive Sciences and Managerial Sciences have regularly emphasized that the exponential growth of information production technologies have significantly enlarge existing gaps between information production and human capacities to utilize this data. In other words, more information production and collection is *anything but* the same as more information semantics and more information semantics is *certainly not* the same as information utilization (Idenburg, 1985; Simon, 1957). While our technologies to produce and disseminate more data in a more rapid way has increased almost exponentially over the last decades, human cognitive capacities to scan and process this data is at best growing steadily and slowly over generations. In other words, even *if* leaders will be able (and are willing) to create significantly more time on the processing of incoming warnings, it is still highly likely that many relevant signals will go blind. This discouraging truth is easily applicable for the subject of this article as well: The gap between what intelligence analysts, as well as military and political leaders know and what they *could* have know given the fact that (in hindsight) the data is or was within their reach is still becoming bigger and bigger (Idenburg, 1985: 5). Sometimes signals will go blind as a consequence of deliberate decisions to concentrate scarce resources on the transcription and interpretation of one type of sources and to ignore other collected data largely (like the decision of President Roosevelt and a small circle of key advisors in the months before the Japanese attack on Pearl Harbor in December 1941 to concentrate mainly on the transcription of “Magic”). The net result may be that policy-makers will frequently be confronted with bigger discrepancies than ever between all data they are exposed to, the information the asked for, the information they really needed (including relevant warning signals and threat assessments) and the data they actually process and utilize. In sum, Francis Aguilar’s conceptual picture about the discrepancies between various forms of intelligence may be more relevant than ever for actual and future situations in which wrong responses to impending dangers can have far-reaching, unforeseeable consequences (see Figure 3).

*Figure 3***:** *A conceptual relationship among different forms of information a decision- maker is dealing with (an adapted version from a idea of Aguilar, 1967).*

Denial and avoidance coping tendencies

Last but not least, the introduction of new information technologies will certainly have an impact on the cognitive appraisals, dilemmas, and coping strategies of political leader's. Given the fact that there are usually many political reasons and practical limitations (lack of resources) why intelligence (such as satellite pictures that of preparations for a large-scale genocide) is not welcome, policy-makers will frequently reveal strong forms of denial and avoidance. “Intelligence to please” syndromes among the leader’s senior advisors, departments and agencies will certainly be one of the major (often frustrating) reactions. It remains to be seen to whether it will makes a real difference to deny and avoid repeating visual pictures in a time wherein journalists seem to be earlier aware than ever that intelligence has been ignored.

THE IMPACT OF NEW INFORMATION TECHNOLOGIES ON AN ACTOR’S PREPAREDNESS ITSELF

Given recent experiences and extrapolating to the nearby future, it is probable that the invention of information technologies and information operations may seriously affect the essence of preparedness itself as well. First, as we have already emphasized, due to their specific character and the range of variations most (if not all) policy makers are likely to have serious problems in attaining sufficient mental and conceptual readiness towards features of the danger itself as well as initiating an adequate response. They will usually experience serious problems in being ready for (a) the occurrence of the offensive; (b) in imagining the type of actions that are going on (because confrontations with such types of dangers are still relatively new in human history; (c) the locations on which the informational technological attack is directed; (d) the timing of the confrontation (because for some types of attack this can be better hidden than ever); (e) its strengths and weaknesses (in comparison with the strengths and the weaknesses of the defense (capabilities, organization, but also mentally); (f) and the specific objectives and consequences of the attack.[6] Second, it is quite likely that most policy-makers will have serious problems in becoming and keeping sufficiently informed about the set of conceptual, physical, and mental components of the “basic measures” and “emergency measures” they may have to mobilize in case of an attack. In fact, being consciously aware of the strengths and weaknesses of ones own potential measures for defense may become a bigger problem than ever before. To oversee the exponential increase in possible variety and numbers of basic and emergency measures, as well as the variety of potential dangers and vulnerabilities is often an impossible attack for experts. So, how will a political leader or a general, who usually tend to at best a small amount of their time and energy to these issues, be able to be ready to oversee them and suddenly base decisions on it in times of rising distress and time pressure? In the third place, it may become more difficult than ever to build up sufficient political acceptability in situations wherein the necessity to counter devastating computer attacks of terrorist units or states as soon as possible with military precision attacks. To response in situations wherein there are still many uncertainties about for instance the motives and identity of the attacker and wherein most of the public, policy forums, as well as the press are not mentally prepared for aggressive military counter measures may confront political leaders with really complicated dilemmas and escalation scenarios that are difficult to control.

CONCLUSIONS

Overall, the following tentative conclusions can be drawn:

- The introduction of new information technologies will lead to a further increase of the number of potential warning signals and threat indicators that will be collected.

- New information technologies will lead to a significant increase of a specific type of potential warnings (e.g. in principle current, observable activities or intercepted communications and documents). However, other types of data that may tell something about the specific features of impending dangers will still be difficult to assess.

- The timespan between the issuance of crucial warnings and the actual attack is likely to decline further. In case of various types of information warfare (e.g. computer attacks, for instance on C4I systems) the timespan may even become almost zero, leaving the defender for a long time after the attack in the dark about questions like whether, where, when, how, why, and with what damage.

- The application of new information technologies will have a profound and ongoing impact with regard to the dissemination of a particular type of threat indicators. Dissemination will go much more rapid. Top level military and political leaders get real-time battle field awareness so that they can judge themselves whether or not, and if so, when, where, how and why developments that can be observed makes it necessary to respond with which kind of preparations.

- The new information technologies may make it possible to work more rapidly than ever through decision cycles and surprise the adversaries with rapid counter measures. At the same time it will create many dangerous traps like unjustified "what you see is what you get" syndromes, "sense of false control" and "micro management". Furthermore, it will create a lot of specific distortions and both information overload and partly overlooked information underload.

- The appetite of commanders for the latest, more detailed information about what is and what will be going on in the immediate future will increase significantly.

- The thorough selection and interpretation of the right signals will suffer from various types of time pressures that are not directly created by the situation in the field.

- The gap between (a) information collection and production; (b) information semantics (interpretation); and (c) information pragmatics (adequate use of relevant signals) will increase further. A lot of collected and available relevant signals will go blind.

- In situations wherein for whatever reason military and/or political leaders are reluctant to act on visual pictures more sophisticated types of denial and avoidance by these leaders will be seen.

- It will be more complex and difficult than ever for most (if not all) political and military leaders to be totally prepared.

In sum, there is a lot to be studied and learned on the impact that the wealth of information technologies may have on various dimensions and types of warfare and crisis management. Besides (or perhaps partly due to) the explosion of new information technologies over the last decades Sun Tzu's 2,000 years old maxim, "Know the enemy and know yourself; in a hundred battles you will never be in peril," still seems to be a challenge for at least decades to come. Technology may thereby be a major help. On the other hand it will continue to place the human decision-maker and intelligence analysts, given their bounded cognitive capacities and constrained freedom of manoevre, for many traps, gaps and puzzles.

REFERENCES

Aguilar, F. (1967), *Scanning the Business Environment.*

Breznitz, S. (1984), *Cry Wolf: The Psychology of False Alarms*, Lawrence Erlbaum, London.

Bosch, J.M.J., *Generaals, geleerden en goeroes: Kanttekeningen bij oorlog, informatie en informatie-oorlog*, Royal Military Academy, Breda, 1997.

Coroalles, A.M. (May 1996), On war in the information age: A conversation with Carl von

Clausewitz, *Army*: 24-34.

Davis, N.C. (Winter 1996), An information-based revolution in military affairs, *Strategic Review*: 43-53.

Handel, Michael (1987), “The politics of intelligence,” *Intelligence and National Security* (October).

Hartog, W.W. & Susan Canedy (1997), “Operations in the information age,” in: Pfaltzgraff & Schultz: 174-185.

Idenburg, Ph.A. (1985), *Informatie-overlast* (oratie), Tilburg.

Kam, Epraim (1989), *Surprise Attack: The Victim’s Perspective* (Cambridge, Mass.).

Leonard, R.R. (1998), *The Principles of War for the Information Age*, Presidio Press, Novato.

Levite, A. (1987), *Intelligence and Strategic Surprises*, New York.

Metselaar, M.V. (1997), “Understanding failures in intelligence estimates: UNPROFOR, the Dutch, and the Bosnian-Serb attack on Srebrenica”, *NL Arms: Netherlands Annual Review of Military Studies,* (edited by J.L. Soeters & J.H. Roovers): 23-50..

Metselaar, M.V. (forthcoming), *Coping with Impending Danger: A Study of Denial and Avoidance of Warnings in Political Decision Making* (PHD), Breda..

Molander, R.C., A.S. Riddile, P.A. Wilson (1996), Strategic Information Warfare: A New Face of War, *Rand.*

Owens, W.A. (May-June 1996), The emerging system of systems, *Military Review*: 15-19.

Owens, W.A. (Winter 1996), The American Revolution in Military Affairs, *Joint Forces Quarterly.*

Sun Tzu (Fourth Century B.C.), *The Art of War*.

Pfaltzgraff, R.L., Jr. & R.H. Schultz, Jr., R.H. (Eds.), *War in the Information Age: New Challenges for U.S. Security Policy*, Brassey's, Washington/London.

Vertzberger, Y. (1989), *The World in Their Minds*, Cambridge UP, Cambridge.

Wirtz, J.J. (1991), *The Tet Offensive: Intelligence Failure in War*, Cornell UP, Ithaca/London.

Wohlstetter, R. (1962), *Pearl Harbor: Warning and Decision* (Stanford, Calif.).

NOTES

[1] This dimensions includes a nation's potential, procedures and mental and physical state to recover quickly from the first hours wherein a danger materializes and unfolds (i.e. phase 1 of a surprise attack) and to mitigate and undermine the sustainment of an attacker's initial achievements (i.e. the second phase of a surprise attack) (cf. Handel, 1984: 230). Some historical events which nicely illustrate the crucial differences as well as the close relationship between both phases and dimensions are: Germany's attack on Western Europe (France, Belgium, and the Netherlands) in 1940, the first days of the Battle of Bulge in 1944, the allied landing on Sicily in 1944, the first days of the Six Days War in May 1967 and the Yom Kippur war in October 1973 in the Middle East. The same three dimensions of (un-)preparedness (including most of its components) can also be applied on most (if not all) cases of encounters with large-scale natural and man-made disasters.

[2] There are many studies in which warnings are defined as a type of information. It should be noted, however, that there are also many studies that define "warning" not as an information but as an activity or a stream of activities. For example, an act of alerting a recognized authority to the threat of a new (or renewed) conflict at a sufficiently early stage for that authority to attempt to take preventive action.

[3] The same tendencies may be seen with regarding of traditional sources of information abroad from ambassadors and military attachés in-the-field).

[4] For example, in the Summer of 1995 the fact that CNN came much earlier with the latest developments in advance of the Bosnian Serbian attack on the UN enclave Srebrenica than most intelligence agencies pressed and frustrated several airforce commanders and UNPROFOR staff members who wanted to react as quickly as possible before it was too late).

[5] This definition is derived from several theorists in the field of disaster studies and strategic surprise attacks. In particular: George, 1979: 12-24; Levite, 1987: 2-3; Kam, 1988: 8; Chan, 1979: 171.

[6] Example given in the first section of chapter 1. For instance, Stalin, complete mental breakdown/surprise.