KALEIDOSCOPIC APPROACH TO SECURITY SHADOWS IN THE AGE OF INFORMATION WARFARE

Deyan GOTCHEV

Introduction

In order to learn the necessary rules of the new era one can not usually skip the long period of disorientation and confusion characteristic of all periods of transition. In this paper society is analysed as a set of interdependent infrastructure elements. Their functional contradictions lead to conflict-crisis-catastrophe (C3).[1] They could involve dramatic shifts in political power and attitudes toward authority, in the means and the burden of conflict and defence. The C3 activity incarnates as information warfare (IW) and cyber-terrorism.

The aim of this paper is to present one idea about the multidirectional holographic-like construction of the IW space. Special attention is focused on intelligence. In order not to loose orientation in "fuzzy" IW functioning one should try to balance among previous experience, hard reason and the feeling of transformation during a self-organising process. The problems of protection in IW are discussed in order to help the military planner not to forget to be on a cool alert and cautiously to search for newly emerging and interwoven features of the information space. According to the comments made in this paper, the commander in future combat variants should not expect to exist and act relying entirely on a "comprehensive, stable, predictable" scheme.

Society

Some societies and cultures have developed considerable infrastructure to support the elements of the social contract between members of the society. A *"dependency infrastructure"* is created for an economy of scale and to optimise the level of complexity in society. Its successive stages insulate the advanced levels from the details of the previous stages. Dependency infrastructures closely parallel a hierarchy

of needs. Elements of the dependency infrastructure include macro- and micro-administration, transportation systems and communication mechanisms.[2]

The infrastructure on which society depends, in sectors such as transportation, finance, energy, and telecommunications, is becoming increasingly automated as advances in information technology open up new possibilities for greater service efficiency. A *National Information Infrastructure (NII)* today is more than just a larger, more modern and complex version of the Roman road and aqueduct systems. All sectors have components distributed over wide geographic areas. The NII sectors are owned and operated predominantly by private companies interrelated with various sector-specific interfaces among themselves, as well as with federal, state, and local governments. Varying degrees of co-ordination exist among providers within a sector, but *there is no complete central authority within or among sectors.* [3]

In the net, a domain of ever-shifting patterns of links and nodes, parties are exchanging things that may either represent the real world, or have no worldly connection whatsoever. The might of the networks comes from their redundancy, or multiple pathways between any two points. Value is added only at nodes. Management of the net becomes functionally based. With secure communications and coherent information sharing, the net's hierarchy and overall organisation have a good memory about the participants and avoid a weak central repository of authority. Immediacy provides that a command is always 'forward'; that's why for a perspective in tactical situation hierarchies should be relied on with great precaution and only temporally.

By using quantitative symbols to represent typical value relations between various resources, the *economy* allows efficient distribution of signals in the social system. Its subsystems carrying representations of situational knowledge may be implemented in both completely automated environments and those involving humans. The information age brings a new level of personalisation to our world that changes the value of consumer products and services. Topologically, the effect of fast signal transports is equivalent to *the collapse of the social space dimensions along established social connections*. We can customise the item to our needs, desires, and even our own physical measurements. No longer do we have to accept the statistical norm. The value added to a product customised to personal preference is the value of knowledge. Now the information-based market can tap this added value.

Today's economic indicators do a decent job in reflecting quantitative changes in the structurally stable areas while using questionable methods to disguise small structural changes as quantitative, and totally failing to account for the new products constituting the essence of real economic progress. As a result, rigorous economic methods become confined to a rapid, relatively shrinking and no longer isolated

domain of stable production, and so *fail to reflect long-term growth* in social wealth, let alone guide it.

For either nation-state or business, private concern to ignore the networked global markets is a risky business, if not impossible. [4] The information age empowers individuals with access, mobility, and ability to effect change anywhere, instantaneously. The value that we place on personalising and individual rights affects the way we view the world and our expectations of nation-states.

The NII components are not synonymous with commerce, profit, and communications. The organisations that have become dependent on the net in order to reduce, if not to avoid, the conflict-crisis-catastrophe triad have placed their trust in the net's systems, even though they are insecure and not always reliable. Data should not be accepted as a mirror-like image of the structure supporting the traffic. Information traffic, partly due to its relatively low cost, often unpredictably becomes inefficient. Whether the forces of the market will continue to provide infrastructure services with acceptable reliability in this environment remains to be seen. [5]

Spurred by information age technologies, our highly personalised social and political processes have become interconnected and non-linear, making it almost impossible to distinguish cause from effect. Consequential benefits of the information revolution include greater economic efficiency, faster growth, demise of territorial sovereignty, and shift of importance to functional power centres and nodes of influence. Our cyber-future will feature direct participation by the individual as opposed to group representation. As a result, *the relevance of authority and sovereignty has diminished*.[6]

The former monolithic threat is now enlarged and complicated by the fast changing diversity of actors, i.e., the increasing role of international corporations in comparison to nations. Coalitions are difficult to construct and even more difficult to maintain.[7] It is impossible to be sure about the direction of these changes.

Conflict is chaotic, confusing, and messy. Internal and expansionistic conflicts have to do with the selection and control over the leverage points of the social contract and dependency infrastructure. The priority of a target is dependent on its value to the other side.

As conflicts migrate from territorial to functional structures, weapons change from guns to words and bank accounts. Virtual money assists economic intelligence and attacks, control of clandestine assets, money laundering, insider trading. Counter-economic espionage is focused on supporting negotiators in trade talks and stopping foreign practices that hurt firms.[8]

Total agreement on national economic objectives is virtually impossible due to the emergent global and networked nature of markets. In the information age *national security strategies will depend less on confrontation with opponents and more on co-operation and trust among competitors*. A sovereign nation might effectively pursue its interests only as it paradoxically subordinates those interests to the common interests of all networked partners. Just like the non-zero-sum game where "win-win" results are not only expected but are required for information-based economies to flourish. [9]

Cyberterrorism [10]

The globalisation and personalising of electronic communications system appear to be undermining the authority of nation-states and facilitating a devolution of power to sub-national and transnational movements, especially those that tap ethnic, religious or cultural loyalties.

As knowledge disseminates the number and locality of the threats and cyber-civil disobedience will increase. "New tribalism" demands for "self rule" and decentralisation gain momentum. The non-state opposition force should be the more frightening potential of IW because of varying motive to target government and civilian sectors, using technology to recruit, organise, communicate, fund, gather intelligence, plan, and even launch operations.

Technology is complex, abstract and indirect in its impact on individuals. It is feared as a result of the following factors:

- the concept of convergence - technology has the ability to become the master and humanity the servant;
- the increase of the "connectivity absurd" according to which the entire world will soon be controlled by a single computer system;
- the sense of chaos and insecurity without computers, their low cost, the opportunity to attack anonymously due to non-specific location make information warfare and information terrorism attractive;
- the means to disrupt or destroy digital equipment are relatively inexpensive, easily smuggled from one place to another, can be used from a distance, and are virtually untraceable.

An unintended consequence of the technological developments is the emergence of new opportunities for terrorists. Because the risk of detection is low, and the risks of apprehension and punishment are even lower, a cyber-space attack can be cheap and rather risk-free. Although less sanguinary, such information warfare type of attack may cause much greater impact.

Furthermore, the aim of terrorism is not to destroy the enemy's armed might, but to undermine his will to fight. *Designed to be feared, terrorism is perceived as being random, incomprehensible and uncontrollable*. These features are in the fundament of its real power. Terrorism warfare is shifting more and more toward civilian targets. Potential targets of cyberterrorism are banks, international financial transactions and stock exchanges, traffic control systems, medication formulas at pharmaceutical manufacturers and power grids. The logic of NII activities makes possible the deliberate abuse such as theft of services and assets, acquisition or alteration of data, corruption or disruption of data in storage or motion, disruption of information services.

Essence of IW

War is a human contest that rewards innovation, learning, adaptability and flexibility. The changes in human society as a whole will entail changes in the way to wage war. The latter are characterised by the use of overwhelming force and a search for technological advantage that is not guaranteed at the commencement of hostilities. IW is a new wrinkle in the geopolitical game -- a game presumably impossible to be prosecuted in terms of the national and transnational architectures already established.

In the current military establishment information warfare is the hottest term used as if it were indicative of something precise and analysable. Information warfare could be defined as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centres of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy those adversary information-based activities thorough command and control warfare and information attack."[11]

The precise meaning of IW is elusive, in part because it describes a wide range of seemingly unrelated phenomena. A central obstacle to a future information warfare capability is that the words and definitions currently used among the armed forces to guide future development in IW are unclear, confused, and often contradictory. For some defence analysts, IW refers primarily to the military application of computers and other information technologies, and the implication for the military establishments of organisational, operational and doctrinal changes. For other writers IW is a much broader idea, relating to the emergence of "Information Age" civilisation and the development of associated modes of political and social conflict which point toward the gradual erosion of nation-states and their monopoly of organised violence.[12]

While information systems are still subject to "territorialisation," *space within modern communication and computing environments is effectively non-metric*, i.e., its dynamics are unlike that of the physical space. Information defies constraint by parameters such as unique locus or finite production. This means that most space-related laws of all previous functional spaces would not apply to "digital" systems. The latter have lower replication costs of agents than execution costs, which makes them dramatically different from all systems more essentially embedded in their physical substrates. As a result, the means for leveraging one's own interests, e.g., tools, tactics, etc., in the information realm will be (or at least can be) qualitatively different from the means applied to leverage the physical space. Another reason for such a focus is that the degree to which warfare becomes innate to everyday life will be directly proportional to the degree to which warfare is conducted exclusively within the information realm. For IW negative experience could not be pre-played in an abstract form, i.e. *time cannot be reversed or compressed*. Another difficulty in information evaluation is generated by the *irregular scale frame of causality*.

Advances in surveillance, communications, and information-processing technologies are all driving the *"Military-Technical Revolution" (MTR)*.[13] Modern society has real-time demands for immediacy. It is required by the change in the range of potential military operations and the constraints consequent of both downsizing and the ever-increasing costs of traditional platforms. In future operating environments marked by ambiguity, speed, and precision effect information warfare breaks the platform-to-platform long-range strategic thinking. [14]

MTR creates the possibility of charging the "information loop of warfare" with unprecedented accuracy and speed, thereby sometimes a possibility of achieving *"information dominance" (ID)* over less capable adversaries. ID is the capability to reshape organisations and revise strategies based upon a systematic analysis of the opponent. ID is the ability to identify vulnerabilities and *centres of gravity* of an enemy, a competitor or even a customer. Where there is cohesion, the analogy of the centre of gravity can be applied. [15] The first characteristic of a centre of gravity is that it remains the enemy's principal strength. The second characteristic of a centre of gravity is that each enemy has only one of them, at least at each war level. The third characteristic of a centre of gravity is that it is the most important one for a given war level and normally depends on the nature of the war itself. A fourth characteristic of centres of gravity is that to some extent they are limited or defined by strategy. ID is achieved by transforming knowledge into capability. The first task in planning for a war is to identify the enemy's centres of gravity, and if possible trace them back to a single one. The proliferation of information technologies has led to the impression that information is itself a centre of gravity. The goal of ID is greater understanding, not total understanding. [16]

Another related concept is that of *Dominant Battlespace Knowledge (DBK)*. In a conventional war, the benefits of DBK are that it removes uncertainty as to whether an attack is underway; gives the location, composition, and status of the attacking units; ensures sufficient knowledge on friendly units. [17] The major problems of achieving *dominant battle space knowledge* are of organising information storage or processing and factorising the decision making. DBK would allow the military to change from a vertical, serial, hierarchical decision making to flattened, parallel, virtual decision making and still be able to turn inside out any potential adversary's decision making loop. A possible exploitation of functional vulnerabilities could be reduced if DBK is built on decentralised decision making.

DBK assumes higher level of situational awareness. Situational awareness has different dimensions, gives the time horizon and the nature of the resources likely to be available, but *"total" or perfect situation awareness is beyond our reach.*

Information about phenomena dynamics deals with dependencies and their thresholds. Dependencies are dynamic and have thresholds. Since the MTR is seen as a long-term process that presupposes threats which have not yet materialised, its relevance to current defence needs is open to question. DBK alone is meaningless. The gap between DBK and actual targeting may require additional local information, man-in-the-loop, or very intelligent weapons with terminal guidance capability. Technology may be pursued to create a force multiplier, but it can also limit opportunity for the development of new ideas or for societal change. Enforced trust in machine data and operation in real-time places human judgement secondary or out of loop entirely.[18]

Information warfare will provide an essential component of the global presence through which national security objectives will be met.[19] As a preliminary step in a state versus state conventional conflicts IW will most likely be used to negate the opponents' weapons-of-mass-destruction, impair their command and control, attack their industry, financial systems, and run propaganda campaigns. This sort of conceptual warfare model by a Pareto simplification is a force multiplier in achieving the intent or mission. Information technology multidimensionality blurs traditional boundaries, changes the whole vision of military operations. *Combat is increasingly assuming the pattern of a continuous flow* rather than a sequence of moves and counter moves. Unlike conventional ways, IW defies the military principle of mass. Its primary objectives are control and paralysis. In future information wars, virtual reconnaissance, strike, and defence would be co-ordinated in battles fought as "meeting engagements" where both sides are on the offence.

Sometimes the narrow margin for the "victory" is based on a very small differential of talent, performance, or luck. It is the relative performance in the above mentioned

activities which makes being "the second-best" (even at lower cost) inadequate. The relative and differential advantage in information, information processing, communications and information security will provide for *asymmetric strategic response* [20] often in the form of Information Operations (IOs).

Information operations' use should be conditioned by operational, organisational, legal, and moral factors. Among the vexing issues is the intellectual separation of the use of force or IO among nation-states, from that in the context of interpersonal relations. IOs can be conducted by other than military means. Some information operations do not involve the use of force: psychological operations, applications of deception, a variety of computer "code bombs," viruses, and "chipping." The more routine "information operations" like "counter-terrorism" can be understood as self-defence not involving use of force.

Unlike economic actions, sanctioning the activities of other states, generally considered as slow-acting and blunt information operations can quickly impose severe damage with low levels of violence. Recently IOs have tended to be judged by the following guidelines governing the use of force: necessity, discrimination, proportionality, and humanity. There have been no specific arms control agreements directed at limiting IOs. In fact, however, with its emphasis on confidence-building measures and operational transparency, arms control has acted to hobble effective information operations. Whether IOs that involve civilian satellite systems are always to be regarded as "non-peaceful" is a fundamental issue that has not yet been settled. It is difficult even to articulate a moral code in such circumstances, let alone to follow one consistently. If, no sort of IO can be brought out from under the "use of force" mantle, for a country with the great capability to conduct information operations, this would forfeit what could be a decisive advantage in peace, crisis, and war.

Information operations have both offensive and defensive aspects and should be fully integrated into overall national security policy. In peacetime they can contribute to the prevention of conflict, or they can be used to respond to crises and overt hostilities. In times of crisis, information operations can be employed to resolve disagreements, fortify deterrence, or prepare for the possibility of open conflict. In war they can directly achieve strategic, operational, and tactical objectives or underwrite other means to achieve such objectives.

Means of Conducting IW

They include: electronic warfare; military deception; physical destruction; security measures. Offensive and defensive information operations can use a common variety of means. The net's functionality without ideology offers prime destructive opportunities. It is a bluff that IW scenarios are being studied at present mostly with

an eye toward defense rather than offence. Information technology is being developed by strategic planners both as an offensive battlefield weapon, and as a weapon for "logistics attack." It is designed to disrupt the civilian infrastructure on which an enemy's military apparatus depends. Offensive actions using information operations include those that move information from one place to another, destroy it, promulgate disinformation, and corrupt, degrade, interrupt, or deny data flows without visibly changing the physical entity where it resides. Possible offensive weapons are computer viruses; logic bombs; "chipping"; worms; Trojan horses; back doors and trap doors. Devices for damaging entire systems over a wide area are high energy radio frequency guns, which focus a high power radio signal on target equipment, putting it out of action; as well as electromagnetic pulse devices, which can be detonated in the vicinity of a target system.

Denial of Service Attacks (DOS) are carried in order to hamper, distort and prohibit access, utilisation, or benefit from material (M) infrastructure (DOS-M). DOS are realised through various forms of warfare which focus on different elements of dependencies in society

Information attack will be employed as an expression of global power made possible through global awareness and global reach.[21] Targeting the information infrastructure (V) IW is rapidly polarising along a massive, sneak (DOS-V/M) attack predominantly as orientation management.

The other direction, *political warfare*, is more difficult to accomplish than DOS attacks. Political warfare creates an alternative social contract and dependency infrastructure and induces their common adoption. This is usually achieved through efforts of subversion, rioting and diversionary diplomacy.

Psychological warfare (psyops) requires a human touch to debase human decisions. Psychological warfare is the attempt to warp the opponent's view of reality, to project a false view of things, or to influence his will to engage in hostile activities. It can be divided up into categories according to their targets: operations against troops, operations against opposing commanders, operations against the national will, and operations designed to impose a particular culture upon another. From a psyops perspective one of the 'problems' of the net is rooted in the users' scepticism generated by their education and experience.

The information revolution has led to information overload, and people respond to this pressure by trying to process messages more quickly and, when possible, by taking mental shortcuts. Propagandists short-circuit rational thought by agitating emotions, by exploiting insecurities, by capitalising on the ambiguity of language, and by bending the rules of logic, i.e. by limited and specifically targeted DOS attacks.[22]

Intelligence[23]

The best weapons, those that make men dangerous, are tools of thought i.e.system analysis, operations research, game theory, cybernetics, general semantics, etc. Iintelligence, is all about information. The more we know about the other side, the more economical our strikes against it can be. Intelligence can be the discovered or acquired variety from espionage and the domain of operations. Cognitive intelligence creates new ways of thinking. The cognitive hierarchy phases are: correlated data becomes information; information converted into situational awareness becomes knowledge; knowledge used to predict the consequences of actions leads to understanding. The act of data gathering should not trigger "Heisenberg's effect" (intelligence gathering effects target). Embedded knowledge is hard, if not impossible, to steal. Operationally speaking, knowledge and understanding of the opposition is the most important sort of information to possess (some even thought it more important to control information regarding themselves over espionage against enemy targets).

For an insurgency to work, there needs to be an alternative social contract and dependency infrastructure established. The net already comprises such a system. Building and testing models is one of the primary functions of the net. This is what makes it such a potent intelligence tool. Game theory can be used to create and test scenarios, for factoring in operational risks and consequences.

Information creates and then degrades *models*. A model is created to answer questions generated by logic. It is artificial and often out-of-date. Models are based on formalization of quantities. During phenomena observations the measured characteristic values become quickly polarised and unstable, even irrelevant to "sound reason", and so new types of numbers are created in an attempt to overcome the paradox. The same is valid for data processing methods. The great obstacle in model construction is the impossibility to create an absolute, universal and final model. This is due to inadequate degree of abstraction based on real observation.

Information mechanisms create new abilities for *deception, blackmail and sabotage*, the creation and manipulation of "truths", through monitoring and manipulating message traffic. Operational organisations will tend to be small, tightly directed, well camouflaged and hard to detect and stop. The information environment can accommodate any number of them 'inside' the same virtual territory. They require a high degree of security and trust- the cornerstone of such relationships is the proper selection of personnel. Weeding out of potential members through a thorough background investigation is possible as never before. The reversal of this process is also important--"legends" can be created and seeded across the relevant databases.

*Counterintelligenc*e must be viewed not as an annoying intrusion but rather as an integral part of the intelligence process. It must focus not only on protecting our own sensitive information, but equally on external efforts to manipulate our collection and analysis. This requires certain openness of mind and willingness continually to balance the conclusions drawn from intelligence with the possibility of deliberate deception by a target. Intelligence analysts who are familiar with the totality of information on a particular topic are often in a position to detect anomalies. This comes from building cognitive models of the objectives, constraints, assumptions, dependencies, patterns, and complexities of your opponent.

In the international community the "slippery slope" of the move to *open source and competitive intelligence* has become one of espionage (by definition espionage is illegal) and sabotage. The net is becoming a well defined entry point to the media cycle. Deliberate sensitive figure manipulation especially in speculative areas like finance, natural disasters, crime and migration extremely hampers noise filtration. The unbalanced presentation and analysis of facts could cause close to fatal deviations in the decision loop.

The net offers unprecedented opportunities for synergism among information-charged paradigm sets like religions, global conspiracies, meta-knowledge, etc.

For intelligence and counterintelligence applications subliminally implanted posthypnotic suggestions and scripts use acoustically delivered and phonetically accelerated posthypnotic commands without somnambulistic preparation of the subject. Additional applications include misinformation dissemination, confusing and confounding leaders during critical decision moments, distorting significance of various facts to sway decisions and actions, behavioural modification and self initiated executions. This technology is used to develop and control spies, political candidates, and other public figures through psychological intimidation, fear and extortion. This technology is the perfect intelligence tool. The subject does not know the source of the technology or the technology itself, the subject has no proof or evidence, only their perception, suffering, and isolation.

Information effects *risk*. For the ease of risk evaluation sometimes the very essence of logic restrictions of the math constraints embedded in the calculation techniques are neglected. The situation analysis is overloaded with psychological and civilisational nuances inconsistent with the embedded calculation technique. This makes the results not-trust-worthy especially for scenarios' crossroads. The societies' multidimensional interactions' non-definable and with a not-fixed topology space of states makes prognosis to surpass a normal challenge. A discussion about the need to use and rely on intuitive para-techniques unrelated to objective schematisation is underway.

Is it possible with responsiveness and efficiency to manage the problem of information synergy and intelligence? In the game of strategies' testing the choosing of the moment to publish/activate pieces if information rarely coincides with the moment of data assessment. Parallel intelligence cells and multi-level not-contacting functional scenarios, tightly compartmentalised information exchange and manipulation with archives' secrecy contribute a great deal to the artificially distorted for political aims picture. As a result of the balance among humint, osint, sigint and imint interpretation new *rules for dealing with "floating" fuzzy truth are generated during real time operations*. Maybe a set of not-contacting, and even contradicting variants represent an alternative for an optimal functional medium.

Protection

Albert Einstein once observed "The Lord God is subtle, but malicious he is not." During information warfare, demand for information will dramatically increase while the capacity of the information infrastructure will most certainly decrease. Critical areas in need of protection are: information, communications, electrical power systems, gas, oil, banking and finance, transportation, water supply systems, emergency services and governmental services.

Is there enough military gain from a concerted attack on the civilian infrastructure to warrant the risks? Considerable interest in the politico-military potential of cyberspace has devolved into planning and acquisition focused on *the integrity of specific nodes* or regions within the realm of perspectives, approaches and tactics. This reduces all of IW to a unimodal defensive posture, i.e. addressing all cyberspace risks through guarding and patrolling those systems within one's own zone of control.

Security and information assurance as it applies to telecommunications in defensive information warfare could be viewed as a classical quality problem. Infrastructure information networks face a lot of *reliability challenges*. Network failures can be classified in terms of the mechanisms by which they are manifested and by their causes. Mechanisms range from chain reactions, in which small faults propagate and result in widespread disruptions, to the direct, independent failure of key components that in themselves represent major disruptions. Causes range from natural disasters to human error, and from equipment failure to deliberate destructive acts by person's intent. From a technical standpoint, these are not different problems; they are different parts of the same problem.

Fragility is an inherent inability, realised or not, to respond to changes in external conditions. In the context of mission accomplishment, fragility is a substantial source of risk, and therefore its identification, reduction and control are critical. Fragility

may occur from either the overt actions of the enemy or the natural occurrences which sap energy and resources during the course of military operations. [24]

We theorise about our own information technology vulnerability and then assume it is the same for others. No one really knows how vulnerable is the national information infrastructure. We do not know what *normalcy* in the infrastructure is and how it varies with such things as season, world events, national holidays, etc. We need to establish the "noise level" in the infrastructure--namely, the day-to-day abnormal or accidental events that occur as a matter of routine operation. At the operational level, network intrusions are difficult to detect because they can disguise as legitimate transactions or go unnoticed in a busy network. In many networks today, successful intrusions are more likely to be detected by their effects rather than by any discernible telltale signature.

The propagating *"chain reaction"* failure mechanism is characteristic of complex systems with tightly coupled subsystems. Seemingly inconsequential events trigger an unanticipated multiple interaction of anomalous operating modes among subsystems. The problems can be exacerbated by the very features and procedures intended to protect against failures. Systems should be designed to be redundant and to fail gracefully rather than catastrophically.

Little evidence exists of *recovery or protection synergy* which cuts across sectors under attack. It is usually necessary to find specific defences against specific attacks. These defences, in turn, become targets for future attack. Currently there is much about this threat that is not known. Currently, the security solutions lag far behind the potential threat. This situation is likely to continue until the threat becomes reality, forcing a reassessment of the preventive measures. [25]

Surprise works because it hits from unexpected directions, forces an unexpected and disruptive phase- change with the attendant loss of coherence while re-orientation is taking place. In information operations, as in terrorism, the possibility exists that a devastating attack will be made without the perpetrator being identified. Even if an attacker can be identified, questions arise about the proper form of retaliatory action. Such questions enervate deterrence by reducing the certainty of retaliation. If one can formulate no appropriate and effective form of retaliation, one is obliged to rely on deterrence by denial. Moreover, because information operations can take place at very high speed and without warning, the implications of surprise are potentially serious at all levels of information warfare. If this distinction about the operational acceptability of information operations is recognised, decision makers must assess the possibilities for the adversary to retaliate, and also they must determine whether they can defend against or tolerate that retaliation.

There are indications that, in order to avoid the inevitable difficulties, superpowers try to test the possibilities of a strategy that shapes the environment. In its preliminary stages the basic efficiency paradigm is suspicious.

We do not possess the omnipotent assessment-decision tools to steer an opponent via ID. Thus, against an adversary dealing with the most ambiguous defence topics, a pre-emptive, quick and simultaneously applied *full-spectrum strike* focused on the very sensitive points of control should not be ruled out, too. The resulting stress for the decision makers could lead to time-disruptions and errors in the planning phase, logic deficiency, paralysis and subordination of will.

Defence-in-Depth is an approach to design, implement, and operate where each and every component, system, subsystem, process, procedure, etc. is looked at to see what threat could occur at that level, and then addressing the threat at that level. The targets' spectrum ranges over international political and economic competition, military operations other than war, crises, overt conflict, termination of conflict, and restoration of normal political and economic competition. Defensive actions seek to protect one's own information frame from similar actions of an adversary and to avoid promoting paranoia and the resulting dissipation of responsibility.

The threat of massive disruption through information warfare has been posited as a potential successor to massive destruction by nuclear warfare. General *deterrence* stems from maintaining the capability and will to inflict severe damage in retaliation against adversaries. Its effectiveness relies on the presence of an arsenal of tangible capabilities. "Focused" deterrence operating by threat of punishment of identifiable targets is "stronger" than general deterrence. Aside from punishment, general deterrence based on very strong defences can work through denial. Since no defence is stronger than its weakest point, the ability of open societies to deter an information attack by a strategy of denial always will be uncertain. Deterrent to information warfare could be economic interdependence, fear of escalation, lack of technical expertise (it is the weakest factor and is eroding fast).

Protection is to be sought through:

a) *Degree of access*. Technology, and especially information technology, is best understood in its societal context. Can the operational utility of the net be limited? People represent both the strongest and the weakest links in the reliability chain. An enemy "mole" with precise and accurate knowledge and understanding of how decisions to respond to a crisis are made and how information is passed within the military might get inside the cycle and do real damage.

Attacking a system whose interfaces are publicly available and thus well-understood is far easier than attacking a system whose parameters and interfaces are proprietary

trade. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. Although 95 percent of US DOD unclassified communications depend on the NII, *the net is rarely used for mission-critical tasks*. An attack on the NII, that left an opening for strategic mischief, could be far more damaging than one that merely caused damage. Co-ordinated cyber attacks are focused, organised, and carefully calculated to yield a specific outcome. The case for assigning cyberspace defence to the DOD arises from the prediction that cyberspace attacks could become the predominant feature of 21-st century warfare.

The net is not the sort of place that can be 'occupied' in a military sense. It could be shut down, but nobody can 'take' the net and hold or police it. The technologies to re-establish it, even in a covert form, are spread enough to make an 'official' shutdown improbable. *For the net to exist, it has to remain freely accessible.* No good alternative exists to having system owners attend to their own protection. Government restrictive regulation of cryptography removes the technology from the legal users, since it is a defensive technology, not an 'armament' as many wish to classify it.

IW opens new opportunities for bureaucrats and "black" programs. The *"privacy versus encryption"* discussion signals that society does not trust the government to fight terrorism. At its extreme end some people are afraid of an elite-sponsored form of new world order imposition attempt.

b) *Resources spent on sophistication*. Infrastructure information networks are inherently dependent on *software*. Every software performance enhancement carries the possibility of introducing logical errors, undoing previous algorithm corrections, changing software and timing performance. It is even possible for malicious code, deliberately and surreptitiously included in critical software during production, to go undetected in installation. All these can increase system vulnerabilities. Competition can pressure developers to rush software to market without sufficient testing. Software-developing companies are increasingly contracting with others, i.e. system integrators are left with little insight into the development and validation of critical control software. Long-term maintenance of software is made difficult by changing preferences in programming languages and lack of support tools for obsolete or orphaned systems.

Some innovations carry new security risks, but the emphasis on adopting today's security practices may keep systems astray from taking advantages of tomorrow's innovation. In security, the primitive is often superior to the sophisticated, but the complexity of systems often constitutes in itself a barrier to attack. A system that is easy to abuse in one way may be difficult to abuse in another. *Heterogeneity* makes co-ordinated disruption harder to achieve and preserves alternative paths. Even

insiders can rarely count on knowing how information is routed into a decision. In an age in which hierarchical information flow is giving way to networked information flow, the importance of any one predestined route is doubtful.

Threats to the infrastructure are challenging existing boundaries between the national defence, intelligence, law enforcement, and regulatory roles of the government. Clarification of missions, responsibilities, and authorities in this new context are needed, and will necessarily involve all the executive, legislative and judicial branches of government.

International law is currently ambiguous regarding criminality and acts of war on information infrastructures. In political science, national security studies have been divided into realism and liberalism. Reality needs non-lethal approaches, reversible effects, keeping open the channels of communication and opening up pathways to conflict resolution. Global liberal institutions and agreements would be a step in the right direction. There isn't any traditional way to dominate, control, protect in the IW space. An alternative, or at least partial, essence core should be integrated amidst the background-level noise, i.e., kept as a back-up copy out of view and reach. Maybe a simplification of clearance procedures will increase security effectiveness. However, we must always accept the realist presumption that information warfare in one form or another is inevitable.

Prognosis

Parallel with IW a new form of "Low Intensity Conflict" emerges. Human tragedies will be used to camouflage truth in power games (e.g. Caucasus, Balkans). Simple facts will be of no help to reconstruct even a possible causality. The technology-empowered media and the proliferation of personal information/communication devices will have the effect of limiting the practical ability of casualty-adverse democracies to engage in combat for much more than a couple of weeks (e.g. UN/US/ "human rights" activities in Africa). Planners for information-age conflicts ought to consider, therefore, training and equipping forces for extremely intense, hyper- or *"blitzkrieg" style warfare flow of combat operations* (e.g. US Marines).[26]

"Low Intensity Conflict" operations cause failure of parts of a dependency infrastructure. Guerrillas and terrorists operate beneath low-intensity conflicts' "sophistication threshold." Especially in the post-Cold War context, few of the small wars currently engage the vital interests of major powers or seem likely to bring about immediate changes in the international balance of power. War represents the most imitative activity known to man. In order to wage low-intensity conflicts with any hope of success, conventional armies may have to adopt the organisational methods, and perhaps even the mentality of their opponents. *Distinctions will thus erode*

between military and police forces, and ultimately among soldiers, terrorists and criminals who are responsible for combating.

While forecasts of a *"coming anarchy" or "clash of civilisations"* may be overdrawn now, war in the Information Age could well spill outside of the Clausewitzian framework where it functions as a "rational" instrument of state policy. Different cultures have shaped war into bizarre and self-destructive forms whose warrior practitioners, unlike modern soldiers, often looked upon combat as a means of self-expression, recreation or religious sanctification. Such peoples are hardly the type to capitulate solely as a result of the "bloodless" information warfare techniques touted by so many as the future of war following the purported "revolution in military affairs".

Information-age warfare will likely see both new techno-weapons and more traditional arms used in *innovative and unexpected ways.* Enhanced communications can release potent psychological energy to produce violent results. It is dangerous to underestimate how significantly emerging technologies will empower warrior peoples. This kind of technology does not depend upon the physical presence of foreign military trainers who might otherwise be able to influence and moderate warrior societies' actions. Some adversaries may abandon whole classes of weapons that require highly trained operators in favour of fully automated, easy-to-use systems. By using technology to replace the intellectual achievement that could previously be obtained only through laborious and time-consuming courses of study, the combatants on future battlefields will become much more equal than has historically been the case.

All generations of warfare coexist, because technological transformation does not occur everywhere simultaneously. As society has become more complex (not even modern), the traditional means for society to police itself have become susceptible to new frailties which at least complicate, and possibly compromise, maintaining that society (e.g. IRA, ETA; Indonesia).[27] In a post-Clausewitzian world war couldn't be clean and short which makes high-tech armies' effectivity doubtful (e.g. US anti-drug campaign in Latin America).

Conclusions

Instead of unrealistic and quixotic seeking of ID on tomorrow's battlefield, the focus must be on developing doctrine and strategies for operating in an environment of "information equality" based more on "information fuzziness" than on partial "information transparency". A main feature will become operation in the obscurant boundary region between real and often not-understandable phenomena and dominating bluff. *The optimal aim should be to try to keep a full-scale and range*

contact with the environment in order at least to define a set of questions for the observed puzzle.

Notes:

1. Deyan Gotchev, "IC3 – The Informativeness of the Conflict-Crisis-Catastrophe Trad," *Information & Security: An International Journal* 1, 2 (Fall, Winter 1998), 43-55.
2. Alexander Chislenko, "Automated Collaborative Filtering and Semantic Transports" <*sasha1@netcom.com*>; Michael Wilson, "Infrastructural Warfare," *Presentation at the receipt of 1997 Sun Tzu Award from the US NDU*, Available at http://www.7pillars.com/
3. John H. Gibbons, Assistant to the President for Science and Technology, *Cybernation - The American Infrastructure in the Information Age. A Technical Primer on Risks and Reliability* (Office of Science and Technology Policy, Executive Office of the President, internal date April, 1997, embargoed until November 12, 1997); *NII Security: The Federal Role* (Office of Management and Budget, 1995).
4. Robert R. Tomes, "Boon or Threat? The Information Revolution and U.S. National Security," *Naval War College Review* 53, 3 (Summer 2000), 39-59.
5. R. H. Anderson and A. C. Hearn, *The Day After in Cyberspace II*, RAND report MR-797-DARPA (Santa Monica, CA: RAND Corporation, 1996); "Science and Technology Assuring Our Preparedness and Improving Global Stability", in *National Security and Global Stability* (Washington, DC: The White House), Chapter 3.
6. Alexander Chislenko, *Some Thoughts on Multi-agent Systems and Hypereconomy* (1997).
7. Alvin M. Saperstein, "War and Chaos," *American Scientist* 83 (November-December 1995), 548 - 555.
8. Nick Kotz, "Mission Impossible," *Washingtonian* (December 1995), 145.
9. Sir Leon Brittan, "EU Pursues Global Answers: International Economic Instability is New Threat," *Defense News* 10, 48 (4 December 1995).
10. Matthew Devost, "Political Aspects of Class III Information Warfare: Global Conflict and Terrorism," *Second International Conference on Information Warfare* (Montreal, Canada: January 18-19, 1995); Barry Collin, "The Future of CyberTerrorism," in *Proceedings of 11th Annual International Symposium on Criminal Justice Issues* (1996). Available also at http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm; *Patterns of Global Terrorism* (Washington, DC: United States Dept. of State, 1996).
11. Randall Whitaker, *Information Warfare* (Umee: Institutionen för Informatik Umeå Universitet, 1998); Todor Tagarev, "Evolution of the Notion of 'Information War'," *Military Journal* 105, 3 (1998), 80-86.
12. Gunilla Ivefors, *Defeat the enemy before battle - a warfare revolution in the 21-st century?* (October 22, 1996). Available at http://www.ida.liu.se/~guniv/Infowar; D. Magsig, *Information warfare will dominate 21st century conflict* (1995). Available at http://www.seas.gwu.edu/student/dmagsig/infowar.html.
13. William Owens, "The Emerging U.S. System of Systems," *Military Review* 75, 3 (May-June 1995), 15-19.
14. Michael Mazarr, et. al., *The Military Technical Revolution - A Structural Framework* (Washington, D.C.: Center for Strategic and International Studies, March 1993).

15. *DOD Dictionary of Military and Associated Terms*, Office of the Joint Chiefs of Staff, Joint Publication 1-02 (Washington, D.C. 1984), 188; Carl von Clausewitz, *On War*, eds. Michael Howard and Peter Paret (Princeton, N.J.: Princeton Univ. Press, 1984), 595-6, 617-9; Lisa Bennett and Bruce Niedrauer, "Center of Gravity," *Military Intelligence Professional Bulletin* (April-June 1995), 25; William W. Mendel and Lamar Tooke, "Operational Logic: Selecting the Center of Gravity," *Military Review*, (June 1993), 25.
16. Owen Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal* 8, 4 (Winter 1994), 35-43; John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review* 22 (Summer 1994), 24-30.
17. Stuart Johnson and Martin Libicki, eds., *Dominant Battlespace Awareness* (Washington: NDU Press, 1995).
18. Paul Bracken, "The Significance of DBK," in *Dominant Battlespace Awareness*, ed. Stuart Johnson and Martin Libicki, (Washington, DC: NDU Press, 1995), pp. 51-65.
19. For a comprehensive study of one particular aspect the reader may refer to Robert D. Critchlow, "Whom the Gods Would Destroy: An Information Warfare Alternative for Deterrence and Compellence," *Naval War College Review* 53, 3 (Summer 2000), 21-38.
20. Richard Szafranski, "A Theory of Information Warfare. Preparing for 2020," *Airpower Journal* 9, 1 (Spring 1995), 56-65.
21. George J. Stein, "Information Warfare In 2025," A Research Paper presented to *Air Force 2025* (Air War College, August 1996). Available at http://www.au.af.mil/au/2025/volume3/chap03/v3c3-1.htm.
22. Aaron Delwiche (March 12, 1995) < *redwood@u.washington.edu*>.
23. John Deutch, "Remarks at CIA Town Meeting," <*http://www.odci.gov/cia/public_affairs* >, (May 11, 1995); John M. Deutch, "Speech at NDU", <*http://www.odci.gov/cia/public_affair* > (June 14, 1995); James Woolsey, on NBC, "The Future Director of Intelligence," *NBC News Transcript* (July 18, 1994), 3.
24. Carl von Clausewitz, "Friction in War," Chapter Seven in Book One of *On War*, eds. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1984).
25. Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *Proceedings of the U.S. Naval Institute* (January 1999). Available at http://www.usni.org/Proceedings/Articles99/PRObarnett.htm.
26. Richard Chilcoat, *Strategic Art: The New Discipline for 21st Century Leaders* (Carlisle, PA: U.S. Army War College, 1995).
27. Charles William Maynes, "The World in the Year 2000: Prospects for Order or Disorder" in *The Nature of the Post-Cold War World* (Carlisle, PA: U.S. Army War College, 1993).

The volume of IW literature is growing quickly. Besides this rapid growth, the duplication of materials among diverse venues (both print and electronic) makes it difficult to track the field. This set provides a compilation of materials established as authoritative sources and reference base for the student of Information Warfare:

- David Alberts, *The Unintended Consequences of Information Age Technologies*, Directorate ACTS (Washington, DC: NDU Press, April 1996).

- John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Foreword by Alvin and Heidi Toffler (Santa Monica, CA: RAND/National Defense Research Institute, 1997).
- John Arquilla and David Ronfeldt, "Cyber War Is Coming!" *Comparative Strategy* 12 (April-June 1993), 141-165. Available at http://www.stl.nps.navy.mil/c4i/cyberwar.html.
- "Operations," *U.S. Army Field Manual 100-5* (Washington, D.C.: 20 August 1982), Available at <http://www.psycom.net/iwar.1.html>
- *Report of the Defense Science Board Task Force on Information Warfare--Defense (IW-D)*, Defense Science Board (Washington, DC: Office of the Secretary of Defense, November 1996).
- Reto Haeni, *An Introduction to Information Warfare* (Washington DC: School of Engineering and Applied Sciences, George Washington University, December 1995). Available via WWW at: http://www.seas.gwu.edu/student/reto/infowar/info-war.html
- Roger Molander, Andrew Riddle and Peter Wilson, *Strategic Information Warfare -- a New Face of War* (Santa Monica CA: RAND Corporation, 1995).
- Stuart Johnson and Martin Libicki, eds., *Dominant Battlespace Awareness* (Washington, DC: NDU Press, 1995).
- *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, US GAO/AIMD 96-84 (Washington, D.C.: General Accounting Office, May 1996).
- *The National Information Infrastructure Protection Act* (1995).
- Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunders Mouth Press, 1995).

DEYAN GOTCHEV: Born 1955. M.Sc. (1980, Physics of the Earth, Atmosphere, Space) from the Sofia University "St. Kliment Ohridski". Research Fellow (1989, Active Experiments) in the Space Research Institute of the Bulgarian Academy of Science. Author of over forty publications in solar- terrestrial physics, synergetics, non-linear dynamics, torsion fields, and fuzzy systems. Besides publications in the mentioned areas, he has authored a couple of papers on crisis management and other interdisciplinary topics. Address for correspondence: Space Research Institute-Bulgarian Academy of Science; Sofia 1000 P.O.Box 799, Bulgaria. E-mail: dejan@space.acad.bg.