DECISION SUPPORT SYSTEMS, inc.

DSSI *METATEMPO: SURVIVING GLOBALIZATION*

WAGING IWAR

MICHAEL WILSON

DECISION SUPPORT SYSTEMS, INC.

INFO@METATEMPO.COM

HTTP://WWW.METATEMPO.COM

Principle and rules in the art of war are guides which warn when it is going to go wrong. – Mahan

INTRODUCTION

So as not to alarm the reader, let me advise you that this paper is intended as an informal presentation of the material, very much in the spirit of 'let us conspire!' What has been sorely lacking in treatments of the infrastructural warfare (IWAR) subject matter has been a practical, personal approach of thinking about, planning, and waging IWAR operations. Given the nature of most of the professionals acting as documentarists, the published materials are strong on theory and speculation, and short on practical guidelines. I shall attempt to begin to fill that gap, and I hope the reader will accept a temporary 'partnership in crime' as we work through the problems facing an opposition force (OpFor) together.

This paper will be broken into four sections:

- Definitions, assumptions, and theory; the conceptual basis of IWAR is important to review;
- Exploration of OpFor as a practical matter;
- A set of IWAR potential operations, for which I have chosen a variety of examples;
- Defense-In-Depth, battling IWAR.

[Being familiar with the Infrastructural Warfare Threat Model previously presented by the author might be helpful for the reader; while not absolutely necessary, it provides certain details which I am omitting in this presentation of the material for brevity's sake.]

DEFINITIONS, ASSUMPTIONS, AND THEORY: A CONCEPTUAL BASIS OF IWAR

He who only sees the obvious wins his battles with difficulty; he who looks below the surface of this wins with ease. – Mei Yao-ch'en

When we consider a subject matter or domain, we think through a problem using the models and metaphors that we have found useful in our own past experience. Metaphors are more an artist's tool–comparing symbols or concepts ostensibly dissimilar. Models are a scientist's tool–a representation of a system, theory, or phenomenon for further study of its characteristics. Both tools are methods for comparing what we are thinking about now with how we have thought about things in our past; the better our metaphors or models, the higher the quality of thinking. As our models and metaphors improve, so does our ability to understand, describe, interact, and define relationships. An example of the benefits of an improved model? Physics: from superstition to Newton, solving certain of Newton's problems with Einstein's work, and solving certain of Einstein's problems with quantum mechanics or superstrings. The improved models allowed advances in chemistry, space travel, electronics, medicine, etc.; the ability of being able to 'context shift' to improved models is critical in deriving the advantages they allow.

What does this have to do with IWAR? Currently, the warfare model is disjointed–there are so many models and metaphors (attrition vs. manoeuvre, mechanized, guerrilla, air/sea/land, etc.), and warriors

can't/don't context shift. A notable example is that of the 'conventional' military coping with non-State actors–e.g., Westmoreland in Viet Nam, a tank commander terribly out of his depth. An oversimplification (but a useful one) of warfare models would be planar, with one axis running from passive to active approaches to conflict ('Doves' and 'Hawks' in Cold War-ese), and the other axis running from a defensive to an offensive posture (defender to aggressor); freedom of movement in the plane is an unusual thing in professionals, military or political. Active/offense is definite, open conflict or war; this is actually a rare thing, as most States and professionals are aware of the variety of costs associated, in lives and materiel. Passive/offense receives very little favorable attention, a form of calculated, potential warfare; this 'war in the shadows' has gained some recognition in recent years as 'low intensity conflict,' or special operations, but the overwhelming negative opinion is still obvious–limited career tracks, public distrust, etc. Active/defense is also very familiar, the assumption that the world is hostile; the active measures commonly adopted are the spiraling arms build-ups that the United States and the Soviet Union both experienced–the creation of a static 'fortress' mentality, with rot at the core. Passive/defense is based on an underlying assumption, perhaps naive, that the world is friendly; notable examples are the recognized Neutral Powers, such as Switzerland or Sweden–open systems until forced to react and close.

Military, political, and social positions tend to lock into such static mindset or 'paradigms'–while the paradigm might be successful given the right conditions (such as the Allied approach in World War II), it becomes less useful as those conditions change (such as in Korea and then Viet Nam, where the application of the same approach foundered and then failed). This is the "if the only tool you have is a hammer, every problem looks like a nail" mindset. The recognition of the dynamic nature of conflict conditions and responses, the switching of paradigms or mental models to address "today's threat today" is critical to waging war upon an adversary; those who can't context shift will fall prey to those who can, as they are capable of shifting the 'rules' of the conflict away from those which their opponent performs well within but are self-limited to. IWAR in fact represents a meta-model that enables movement from conflict context to context while preserving and expanding a warrior's ability to engage an opponent.

IWAR DEFINED

IWAR is nothing new, nor is it particularly a revelation; it is an abstraction drawn from the process of history: conflict oriented to or from the infrastructure of a society. A simple turn of a phrase, but it allows an ordering of conceptualization regarding conflict that acts as a powerful cognitive tool for looking back on the past or planning for the future. After all, why attack military targets? They are 'hard' targets indeed. When what matters is achieving the objective, the goal is military or political effectiveness, and mass materiel does not automatically translate into effectiveness.

In a very real sense, politics is about who owns and controls the infrastructure of a political economy–political systems vary, but the degree of State ownership or control of a social structure is the defining factor; democracy bestows ownership upon the individual; communism and socialism grant ownership to the collective; fascism, dictatorships, and monarchies place ownership on only a few 'special' individuals. The 'rules' of operation in the political economy are defined by the 'social contract,' written (as in the American Declaration of Independence and then the Constitution and Bill of Rights) or unwritten (as in the Victorian 'code of behavior' which pervades the British system to this day). It is therefore no wonder that conflict orients around infrastructure–it has been the means necessary to wage war as well as the prize to be won.

INFRASTRUCTURE--MATERIAL AND INFORMATIONAL

The way in which we categorize society and social structures is defined by developmental level of the infrastructures; elements of the social support fabric that manage and channel materials I will refer to simply as the infrastructure, and elements oriented around more incorporeal components will be

referred to as the infostructure. Obviously, a clean break or distinction between the infrastructure and infostructure is impossible, as the interdependence of the two prevents them from being truly separable.

What might be termed 'primitive' society is agriculturally oriented; more advanced societies, what we now term the 'developing' world, are industrially oriented; and our modern societies are technological; each step in the evolution reduces the importance of the previous stage, but does not obviate it, and all of these societies are still represented in today's global body politique. Advance from one stage to the next, more advanced one is not through a simple, single advance, but more an aggregation of a number of advances–tools, processes, and knowledge that lead to more complex tools, process, and knowledge, all continually becoming ever more complex. If one were to categorize, there are many potential methods of distinction (including the agricultural-industrial-technological one already used), all of them just as arbitrary. As applicable and valid would be to think of primitive societies being those focused around production; increasing demand for energy would lead to a move from animate power sources to inanimate (as in the industrial revolution); concentrated power sources would drive a need for control (leading to the modern world of technology and cybernetics); and currently social pressures are working on the issues of scale and speed (whether at the 'national boundary' level and the erosion of distance as a factor; to speeds in travel, communication, and computation; or in the coming advance toward biotechnology and nanotechnology, or space exploration).

Each level of development, each level of society, has its own mechanism of establishing an information environment or 'infosphere'–in more technological cultures, this environment is enabled by the information infrastructure (infostructure, that specific subclass of an infrastructure), but the information environment is not unique to advanced cultures, quite the opposite in fact. The infosphere is a sort of 'community memory,' the aggregate sum of human knowledge–collectively we know more than we do as individuals. A primitive culture may have to rely on oral tradition, making the infosphere very 'localized' (and which has a tendency to go hand-in-hand with the religious structures of a society) but that does not necessarily mean unsophisticated; as cultures advance to a developing, industrial orientation, the infosphere relies on the broadcast medium, and lends a homogeneity of language, symbols, and aggregate symbols (concepts) to a large number of people. The differences and benefits of this are striking, as a look at the impact of the British or German educational systems upon military prowess, industrial advance, and cultural export demonstrate historically. Common familiarity and ability to 'shorthand' complex concepts with a simple turn of a phrase–a Trojan Horse, Horatius at the bridge, Hannibal crossing the Alps–cannot be underestimated. Modern communication technology has created narrowcasting through the broadcast tools–use of the diverse experience but common symbol set, and appealing to 'niche' categories in a society.

To a differing degree of success, infospheres (of which the infostructure is the transport mechanism) are the mechanism for storage, exchange, and transformation of data into information into knowledge into wisdom–a 'value chain' that provides value-add with each transformation, just like a factory takes in raw materials and turns out finished goods. I won't labor this point, although it is important (in fact, see the relevant comments regarding financial IWAR later in this paper). Data is a 'raw' state generated by experience that becomes information through a process of filtering or exclusion, the arbitrary drawing of boundaries for sets, with any difference that makes a difference being the distinction. What many people refer to in advanced societies as the Information Age clearly isn't–most of what we move about is data (after all, humans do the filtering), or information in only the most basic sense that we're limited by our sensory-proxies in what we can 'record' and shuttle about on the transport layer. Information becomes knowledge when subject to analysis, generalization, utilization by application, and abstraction. The more nebulous and difficult transformation of knowledge into wisdom comes from a deep understanding of concepts and systems, relationships, interactions, and their integration. An example might help clear up any confusion: the act of watching a rock fall is data, being experiential; measuring its fall into discrete units of space and time sets a distinction and creates information from the data; consideration of the information to conclude the constant of gravity, or generate an equation

to manipulate the information is the creation of knowledge; extrapolation of these basic principles (after recognizing them as such!) into an understanding of celestial or atomic motion is wisdom. The data (watching the rock fall) transformation into information is one of content/context (the differentiation of the specific instance of the object from its environment over a discrete unit of times); information into knowledge is intra-contextual (an understanding of the meaning of motion and a mathematical definition based upon the rock's motion in the environment, all bounded inside the same conceptual 'set'); knowledge into wisdom is inter- or meta-contextual (application of the knowledge from one conceptual set, the rock's motion, into other sets, like atomic or celestial motion). The actions of material and 'information' transformation are key elements of a political economy, and merit some comment–political economies and social contracts are dynamic processes, and these are the building blocks of their construction.

The function of the material value chain (as characterized by the structure and output of the material infrastructure) was actually well defined by John Locke's definition of property–the act of laboring to convert something from one state to another. An individual may pick up a piece of flint, making it theirs by taking it from nature (see the interesting 'property as theft' arguments of Locke's period) and chipping it into an arrowhead; this can be traded to another who makes arrows; and again to another who hunts; the animal brought down by the arrow enters the value chain–literally as 'raw materials' of meat or hide, then finished products; and so on. Each step changes the 'state' of the property, and increases its value or utility in some meaningful way. The 'primitive' social structures are full of easily discernible value chains–farming, metalworking, woodworking, hunting/gathering, etc. Interlaced throughout the material value chain is a second value chain–the informational. Blind labor may change states, but only directed behavior and labor can provide 'value add' (something Karl Marx missed conceptually). It is these two value chains, the material and informational, and the interaction between them, that have advanced society. By accident or design, 'progress' is made; differentiation occurs and must pass through a variation of natural selection–the survival, continuation, and propagation of advantageous variants. From our distant historical perspective, we define progress and the level of civilization by the depth of structure, differentiation, complexity, and specialization in the value chains. 'Primitive' cultures have relatively simple value chains, while modern cultures have such complex networks that they resist static conceptual mapping. Certain advances have a 'threshold' quality to them, where a seeming boundary minimum is passed that redesigns society and triggers a new burst of progress–from 'anarchy' to Agrarian society, to Industrial, to Technological. The Marquis de Condorcet believed, after looking at the application of probability theory to natural and social sciences, that society can be continually progressed and improved. This human drive toward greater complexity, creativity, and adaptability is like Henri Bergson's *elan vital*–a vital impulse for progress, novelty, making things better, faster, cheaper. And this leads to the next piece of the political economy–dependency infrastructures.

Progress is all well and good, but individuals still have basic needs to take care of. A.H. Maslow observed that behavior is purposeful and directed–there is a reason why humans act the way they have and do. Maslow mapped out a hierarchy of needs that direct/motivate behavior and require fulfillment: physiological needs (survival, food, drink, health); safety needs (clothing, shelter, protection); affection needs (family, belonging, companionship); esteem needs (self respect, achievement, appreciation); and self fulfillment needs (realization and utilization of one's potential). As society progressed, grew, and became more complex and specialized, individuals no longer had the time or ability to handle their needs personally–but they still had needs. Progress took care of this as well–while society went off and advanced in every different direction, certain parts always remained specialized in providing for those needs to be met. These supporting infrastructural segments of the political economy are a continual link down the value chain; no matter how scientific or automated, their nature is essentially the same as established millennia ago.

Supporting infrastructures quickly gained an economy of scale–a favorable ratio of cost of materials to market demand. By providing the necessities or services essential to allow society to function,

infrastructures allow individuals to devote more attention to their own specialization; the freed energy or 'surplus' capital (profit) can be used to fuel further progress. A delicate balance has been struck, however, in the social contract–by specializing and becoming mutually reliant, numerous internal dependencies have been created in the system. It can be like a river that local wildlife depend on, but that goes dry by accident or design; soon there is a diseconomy of scale, with a scarcity of materials (potable water, food), too much competition for limited resources, and a population too large to adapt to the change. What occurs next is a 'die back' to settle with the law of the minimum–the resource most needed and in least supply limits the system. Dependency infrastructures provide the needs and services that keep a political economy functioning and progressing. Primitive cultures, with primitive value chains, have dependency infrastructures that are nearly identical to Maslow's early hierarchy. More differentiated cultures, however, have complex networks for their value chains, so it is difficult to establish a clear 'degree of separation' for the dependencies. Progress has its price.

One element of this progress has been the formalization and specific differentiation of the infostructure, and considerable modern technology is oriented at 'data at rest and in motion'–the consensual hallucination known as the Internet or 'cyberspace' that has become a distinct and increasingly important part of the information environment. The role of information technology in the infosphere is rapidly altering the way society functions–for good and ill. There are increasing dependencies in process and decision; there is decreasing importance on knowing something as opposed to knowing where to find something; reliance on data representations that don't make sense out of the machine has impacted the communication network, financial industry, etc.; an abandonment of understanding processes in favor of getting solutions, like calculating square or cube roots on a calculator as opposed to knowing how to work the problem, not an issue until you have to encapsulate the process rather than just get a solution; the process of qualitative augmentation hasn't truly begun–are the machines making us smarter, or just amplifying us, foibles and all?

The reliance upon the existence of the information transport layer–phones, broadcast media, networks, etc.–are obvious in the business process; what is not well understood, at least in the main, are the more complex dependencies woven into even these services. Vast routing/switching networks that make voice or data transportation possible are based on massive models in multiple dimensions that, even if fixed into a static form temporarily, are beyond human capability to manage or update in real-time; financial models used by nations or corporations are similarly machine-dependent, meaningless without the enabling technology that underlies them, allowing them to function as well as remain dynamic and current. At the same time that use of such complex processes and processing increases in dependence, there is a distinct tendency to not only just rely on the output, but lose access to the skill set that helped develop the models in the first place; in particular, note the tenuous grasp the United States holds in information technology, coupled with its increasing slippage in technical (mathematical and scientific) education. Introduction of computer technology into the classroom certainly doesn't help, and in fact exacerbates the situation; using a computer in early education turns the student from knowing things (processes, facts, concepts) into knowing where to find things, not knowledge at all (certainly not sufficient for the independent comprehension of concepts, understanding the relationships between concepts, and derivation or discovery of new ones). Computers, it must be remembered, need to be explicitly programmed for them to perform any function, which requires an understanding and quantification of the process being programmed.

It is worth noting, and should be no surprise then, that some of the first individuals with cyberspace as a dependency and component of their information environment were those of the U.S. government; it could also be argued that for being the first there, they have managed to do the least with it. Much of the technology and hardware/software backbone was conceptualized, developed, and implemented on the federal dollar, for the intelligence and military community–from satellites to packet switched networks, cryptography, databases, etc. It is too early to tell whether their exploitation of the advance was squandered during the Cold War, or merely a case of pioneers not always being settlers.

Political economies in modern society are built upon these foundations: the material and 'informational' value chains, which then feed the material and virtual dependency infrastructures; advanced, complex societies need this level of specialization and economy of scale to support the function of the social contract, and provide the additional energy or profit that allows risks to be taken, such as new products and processes, new markets, new technologies. Yet the very strength of the system in supporting the social fabric or social contract is the origin of the system's frailness; the empowerment of the individual has meant just that.

The modern social contract is weaker than ever, witness the common breaches and violations by: mentally ill who don't understand the 'rules of society'; criminals risking for profit; those with nothing left to lose; those for whom the contract has failed; those who think the boundaries established by the contract don't apply to them. There are also men of will, driven to change, acting as guerrillas or terrorists. Most striking of all is the level of negation of the social contract by 'ordinary' people; this is not just a feeling of being disenfranchised from the political process, upset with 'private law' or privilege supplanting equal treatment, but outright hostility with a distinct Lockean 'dissolve the contract' flavor. Because of the massive upheavals caused by technological advance, social pressure, regional/ethnic conflicts, etc. the social contract is in flux, on the verge of being 'renegotiated.'

Violence, of course, is how you jockey for position; the ability to destroy has become equated to control. Strong parties get to dictate terms to weak parties; negotiations only occur between equals; peace and stability only happen when the terms are agreeable to all parties of the contract, otherwise the violence continues. The 'defining down' of the capacity for violence has put the capacity to demonstrate dissatisfaction with the social contract available as never before.

On a larger scale, society has hit one of those threshold points again. The rules established and reasonable under the previous phase of development are constricting or no longer satisfactory to many: the consolidated ownership or control of assets in the world economy leaves many feeling the playing field hasn't been level; property and criminal laws are being shaken up by the information age, with digital copying, electronic distribution, industrial espionage, information warfare; overburdened legal systems are incapable of keeping pace. Capacity for destruction has dramatically outpaced moral development: conventional weapons are available or can be manufactured at home with instructions from a variety of sources; weapons of mass destruction, including nuclear, chemical, biological, and informational are devolving down into the hands of organized forces or individuals; the willingness to commit atrocities even now remains only slightly below the skin of the human animal, witness Bosnia or Somalia, as well as victims such as the Kurds or the Palestinians. Dependency networks or infra/infostructures are more vulnerable, interdependent, and already stressed by the needs of society. It is at this point that reconsidering the interplay of the elements of political economy and conflict become critical–whether to hold the fabric of the social contract together, or negotiate a new one.

WHY IWAR EXISTS

Societies and political economies advance, but not according to a design; the 'organic' growth and progress is a 'random walk,' and as such, many of the structural elements viewed as foundations contain a wide variety of conceptual weaknesses and flaws. Social structures and markets adopt de facto standards through momentum and mass–an 'installed base' of adherents, users, believers, supporters, all of whom affect a marketplace disincentive or reluctance to change the status quo, even if for the purposes of correcting problems, such as securing and protecting the social fabric.

Just as all warfare is about infrastructure, IWAR is specifically about attacking the processes (it may be useful here to suggest that the reader think of concepts such as 'terrain,' societies, or people as processes, verbs rather than nouns) or process models in the infra/infostructure, or more subtle attacks that pervert, corrupt, debase, or take advantage of the decision models. An understanding of the technology of control (cybernetics) is particularly useful, but can be quickly summarized–while muscle power is under the direction of a mind (albeit animal or man), inanimate power sources required the

creation of similar mechanisms that could control the greater stored energy. Such controls require a smaller, simplified model of the system to be managed or governed; mechanical computers such as gear works, or advanced computers such as those in service today, provide that process control or governor, and act as the modeling tool necessary to allow automation of various sorts. Application of these modeling tools has expanded from process control into decision making–in two dimensions (big, dynamic pieces of paper; applications such as word processors and spreadsheets) and in three dimensions with time as a factor (complex space/time models; used for designing buildings, automobiles, nuclear weapons; or modeling the weather, global communication routing, financial markets, etc.). Technology for data and information processing is being used for calculations, simulations, databases–things that we might be able to do 'by hand,' but that is becoming increasingly unlikely, or as in some previously mentioned cases, already improbable. As the reliance or dependence increases, so does the trust factor we place in these technological affordances–we know there are mistakes, we know there are errors and failures; yet we willingly believe (almost without question) what we are told by a computer (with no confirmation or authentication, with the 'reputation capital' favoring the output of the computer, however egregious), routinely substituting human judgment and experience with automated decisions, and forgetting that extrapolations or numeric models don't replace the engineering rigor of "you haven't done it until you've done it."

IWAR takes advantage of and targets the frailties, shortcomings, and defects that have occurred as society evolved; it can be waged at any time, in any place, against any culture, and under any circumstance–even the most primitive of societies has infrastructure (by definition), and dependency is such the prevailing circumstance that it has become almost unnoticed. Attacks which deny a society or subsection of a society access, utilization, or benefit from an infrastructure in whole or part are referred to as 'denial of service' attacks (for the material infrastructure, I will refer to them as DOS-M attacks); similar attacks on the infostructure are possible as well (and will be referred to as DOS-V (for 'virtual' infrastructure) attacks). DOS-M attacks vary from the blowing up of bridges or communication switching centers (more advanced societies) to mass attrition attacks on civilian populations (in societies where the people are the infrastructure, such as agrarian-oriented economies). DOS-V attacks, recently being termed such things as 'information warfare,' 'netwar,' or 'cyberwar' can be hackers shutting down traffic control, attacking the software that controls telecommunications switching, or mass flooding of the networks which manage social processes; attack tools can vary from live 'cracking' of systems to automated attacks with computer viruses or network-packet flooders. The intent of IWAR is effectiveness in the attack, and the method of denial will vary with circumstance; regardless of the specifics, iwarring in this fashion upon a target is intended to force failure in a process, or the control/automation of that process.

Rather than outright (and not terribly subtle) destruction/denial of an infra/infostructure, perversion or corruption attacks can target processes (whether material, virtual, or human) and decision processes (and thus degrading the options or recommendations they provide); or impair/damage models, where errors cascade and propagate throughout the model, not always in obvious ways. These psychological warfare sorts of attacks (which I shall refer to as psywar) are far more difficult to accomplish–it requires a human touch to debase human decisions; however, the modern society has real-time demands for immediacy which increasingly force automation of decisions, placing human judgment secondary or out of the loop entirely, trusting in the machine data and operation in real-time. Dependencies are dynamic, and have thresholds–alteration of a medical record to change a blood type doesn't impact the individual until that piece of information becomes critical to making an accurate decision; this means such attacks can occur on systems or information while unprotected because at the time of the attack, they seem unimportant or inessential, an incorrect assumption.

Finally, there are numerous contributions that information technology makes to the process of political warfare–propaganda, disinformation, agitation, and social subversion. This variety of IWAR (which I shall refer to as polwar, a specific subclass of psywar where the subversion is directed at the political process) is a case of "politics by other means"–one of the keys to making changes in a society

or political economy is to create and provide an alternative, gaining adherents through persuasion or compulsion, or by 'forcing the hand' of the existing structure into making reactive changes. The modern infostructure already provides numerous mechanisms for the creation, support, and proselytization of 'intentional' communities (those created by design, such as the 'United States of America' or 'cypherpunks'); technology tools and communication channels provide unparalleled tools for the creation and dissemination of propaganda and disinformation, organize groups, coordinate actions, and otherwise subvert the stability of the social structures.

As previously mentioned, no society is immune from IWAR actions; they can be waged from within or from without, and the tools, methods, and cognitive models are usable cross-boundary–allowing a context shift to iwar in varying modern, developing, or primitive societies, and from one sort upon another. The IWAR cognitive toolset (call them 'conceptual armaments') even lends itself to a sort of 'ontological judo'–a more primitive opponent can use the 'strength' of their more advanced (thus more dependent and vulnerable) foe against itself.

IWAR is not now, however, a ready tool in a State versus State conflict, and I view these sorts of conflicts as being the exception rather than the rule. States have a wide array of capabilities to decide their differences, far less trouble to resort to than warfare overt or covert. Additionally, democracies have yet to war on democracies, and there are an increasing number of ostensibly democratic nations; internally to democratic nations, IWAR is a potentially 'high' level-of-effort course of action in systems where the process of change is already built into the system's political process. That does not preclude use of IWAR, however; after all, non-State groups can effect change through IWAR on the political process in a way that other State actors cannot. A case could be made that the rise of the democratic concept is congruent to the rise of the power of non-State actors–the democratic ideal pushed the authority boundary down just when force capacity also came within the means of the individual or organization. Power and authority have devolved from the State; it was only a matter of time until the prerogative of waging war or engaging in conflict acted similarly.

DEFINING THE INFRASTRUCTURE AND INFOSTRUCTURE

Obviously, infrastructures and infostructures are critical not only in how we define a social structure or political economy, but to their continuing function. There is not, however, a way to universally define the infra/infostructure–dependency is a personal, individual-centered concept that we all have and all generally ignore having. Dependency networks are process networks: dynamic over time, condition/threshold, location, individual, and society.

A useful exercise to gain an understanding of dependency networks (another way of looking at infra/infostructures) is to perform a 'day in the life' analysis; while educational for an individual, a broad study helps to define a statistical pattern of the dependency network process parameters. The act of 'network building' is fairly simple–recording the usage of any services, processes, mechanisms, information, objects, etc. (in short, all material and informational resources the individual comes in contact with or uses) that did not have their origin and owe all of their function to that individual. In a single day in an advanced society, any random individual will have hundreds or thousands of instances–from the bed they slept in, the time on their clock, the power in the light they turn on, to the name they call themselves, and the information and knowledge in their mind. Even the most innocent of objects or actions dangles a deep network of connections–people, processes, tools, knowledge–all of which dangle their own networks.

Performing this exercise on a larger scale helps define, within a rough tolerance, a dependency network. A large body of individuals could perform the 'day in the life' exercise and allow such data to be collected (the period may be longer than a day, in fact). The sample set is going to grow, as this process continues recursively until any utilization of a person incorporates that person (or a reasonable replacement) into the sample set; this first stage (zero degrees of separation) expands, incorporating in individuals who act, in some small or large way, as a resource in the dependency network (note that

these additions are a potential indicator that you've identified a threshold/variable condition--for instance, the use of emergency services like physicians, police, fire, etc.). A distinction should be drawn at this stage that leaves only people in the zero degrees of separation set, and moves everything else into the first degree of separation set. Now comes a labor-intensive task–all of these first degree dependencies are researched to establish their own dependencies, such as manufacturing, skilled labor (which get tossed back into the zero degree set), resources, tools, components, etc. The output from this stage provides a set of dependencies at the second degree of separation; a similar task is performed to establish further degrees of separation, limited only by the efforts and resources of the researcher. A powerful tool–that of 'net-based open source intelligence' (which I quippingly refer to as NOSI)–can make this job in advanced, open societies much easier. Various public databases and resources are available for tracking ownership, function, relationships, work processes, etc. that exist in a functioning free-market political economy.

What the 'end result' of this undertaking provides is a database, manageable by degree of separation, of the dependency network (actually a static representation of an instantiation of the network, and one which requires continual updating and maintenance); the network is anchored at one end by the people who acted as the seed group (zero degrees of separation), and extends out to nodes in the next degrees. Commonality of dependency is evident in the number of links to the same one-node from the zero-set, and then onward through the network–the more instances of links, the greater the dependency on that node (some abstraction would help as well, where slightly more broad categorization will channel into a conceptual as opposed to a specific framework–e.g., the set labels 'physicians' or 'police' rather than specific individuals), providing a 'snapshot' of some of the key points, check points, choke points, and bottlenecks in the dependency network.

The IWAR application of all this effort? Once you have conceptual and specific dynamic models, you can navigate backward and forward in the network of links through the degrees of separation; these models allow an iwar strategist to make target selections by region, domain, or demographic; or pick tactical weaknesses (or targets of opportunity) and then track the consequences (the collateral or cascade effect of the denial or debasement) of IWAR operations. Identification of dependency is critical in IWAR–attacks on non-dependencies have little effect, like using carpet bombing in Viet Nam; if there is any 'diversification' by the opponent, leverage is reduced or non-existent. Dynamic dependency networks are also scalable–identification of dependency regardless of the opponent being an individual, organization, corporation, or State government.

IWAR in all its variations--DOS-M, DOS-V, psywar, polwar–orients around an understanding of dependency infra/infostructures and attacking or taking advantage of their fragility, which is why mapping is an essential process, and an on-going one. Yet while dependency nets are an interesting and useful cognitive tool/resource for anyone waging IWAR, it is only one small component in a quite complex organism, as we shall see.

OPPOSITION FORCES (OPFOR) AS A PRACTICAL MATTER

> *Limited forms of war can no longer be seen as evidence of limited aims: they have become tactical means towards strategic ends.– Maurice Tugwell*

[While discussing OpFor, I find it difficult to maintain a carefully neutral tone; some sections are going very clearly to favor OpFor, a reflection of my own discoveries from practical field experience as a team component and team leader. If you find this disturbing, let me remind you that, in many ways, the intent of this paper is to present the reader with the opportunity to peer inside the mind of an operational individual.]

WHO IS OPFOR?

OpFor comes in many 'flavours' and needs to be looked at segmented by the individuals who comprise it, the intent which shapes it, the ostensible form it takes, and its operational method.

Categorization of OpFor personnel could be managed with the three 'P's–Political, Profit, and Pathology. Political motivation comes from an ideology, a desire for power, or a drive to gain media recognition for an issue; 'good' or 'bad' is entirely relative, depending on which side of the issue you might stand, so no generalizations should be made regarding the moral nature of this motive. Profit motive is fairly clear, or is it–after all, if someone acts in a way that clearly does not profit them, we consider them an ideologue (derisively) or fanatic, yet we also deride the converse. Pathology encompasses radically different issues–revenge, passion, chaos for chaos sake, a need for group identity, having no alternative. Finding 'pure' examples of motivation is atypical; for instance, professional warriors are certainly mixed types, as are assassins. This flies in the face of recent efforts by many parties to 'profile' the psychological make-up of OpFor personnel, whether for law-enforcement identification purposes, or in some measure to 'prevent' them from occurring (a level of social interference that has staggering implications indeed)–the motive behind profiling is either misguided or disingenuous, and the effort dedicated to it better utilized elsewhere.

OpFor intent extends the patterns set down by the individuals–groups assembling for political, profit, or pathological purposes. What sets these groups apart from 'conventional' organizations, such as political parties, corporations, or support groups? Less than you might suppose, which is why the thin line that separates one side from the other is blurring or being erased–social convention, 'arbitrary' legal definition, etc. OpFor can be the whole or part of any scale organization–State, corporation, 'affinity' organization–linked by a common intent, which could be the total destruction of another State, putting a competing corporation out of business, renegotiation of the social contract (entirely or only terms of it), or ruining the life of another individual. Regardless of the stated or unstated intent, function drives form, and form drives function–once an intent is established, appropriate resources need to be marshaled, plans made, conflict begun.

State or State-supported OpFor goals might be political (International Marxism/communism, which subsequent records have documented was supported by the Soviet Union), religious (such as with political Islam), ethnic or racial (such as in the Balkans, or throughout much of Africa), or territorial (which, contrary to surface impressions, describes Ireland and Palestine). Non-State actors, a curious term for what are actually the greatest category of OpFor, may be corporate or focused on corporations (industrial espionage, environmentalists, or 'equality' activists with racial or gender issues), political (attacks to/from political parties, militia movements), ideology (animal rights, anti-abortion activists), criminal (trafficking of various sorts, money laundering–note that these sorts of activities may not be just the mindless pursuit of money, but the view of money or finance as a weapon, discussed in detail later), or individuals (revenge, 'identity hacking,' or assassination of key personnel).

Operational method for OpFor is no light undertaking–each has requirements, skillsets, moral questions. DOS-M attacks require a willingness to take real world risks, not to mention potentially cause real world casualties; the more advanced the society, the lower the tolerance for actions which cause the loss of innocent human life, making most such OpFor actions intending to gain sympathy for the cause moot or counterproductive with the first casualty. DOS-V attacks require a minimum level of technical sophistication, or access to such sophistication; as recent attacks have demonstrated however, that if only for sheer nuisance value, these sorts of attacks are effective (even with automated and limited attack tools). PsyWar requires an understanding of how the decision model or process under attacks works; the more sophisticated the target, the more domain-specific and difficult the attack; additionally, as decision models are commonly attacked long in advance of a dependency threshold or boundary condition being met for the distortion of the process to occur, this also takes a great deal of patience and care, and involves considerable uncertainty. Polwar is, oddly enough, becoming a more frequent occurrence–as the conventional political process degrades (yes, the usage of the psywar term is intentional, the political

process is under attack), it slides farther down the slippery slope, where propaganda and disinformation, agitation and rioting, and other subversions of the political process are regular occurrences. No particular relationship exists between the scale of the OpFor (State through individual) and the operational profile (DOS-M/V, PsyWar, PolWar); in fact, flexibility is essential.

[Many of the next points–recruiting, organization, funding, armament, intelligence–are covered in more detail (including technical) in my previous paper Infrastructural Warfare Threat Model, and I refer the interested reader to the relevant sections.]

Recruiting members into OpFor should be more difficult than it is, but the fractionalization of most societies into affinity or special-interest groups has collaterally acted as a first-pass filter; from there, it is merely a case of sending and receiving signals in the infosphere, and letting narrowcasting do the rest of the work.

Organization of OpFor could be tight or loose; management and coordination are certainly going to vary, and the use of a technological communication infrastructure will reflect these choices. It is worth noting an important cognitive distinction between OpFor for IWAR and other sorts of OpFor: hierarchical organizations of all sorts orient around a monopoly. That monopoly may be of force (as in 'gunpowder empires'), information (particularly in intelligence organizations), command (as in military or political structures), benefit (family or religious structures, where the hierarchical control comes from the ability to dispense food, wealth, etc.), interpretation (as in the Soviet State, which was the arbiter of the dialectic), etc. Monopoly reservation or control of some resource automatically equates to a dependency; IWAR OpFor, being intimately acquainted with the weaknesses inherent in dependency, would show a profound tendency to avoid hierarchies and monopolies, favoring instead a heterarchical relationship with independent (and thus redundant, diversified) information, resources, and command.

Funding for OpFor is almost an afterthought (except in the special case of financial IWAR, covered in detail later); proper selection of a target in the dependency network provides considerable collateral damage (leverage), minimal resources, and manageable risk. OpFor does still need finance though–even if not using money as a weapon, money provides options, acquires resources, purchases training, opens doors, buys information, etc. Sponsorship for OpFor is a double-edged sword–a dependency, intent set by other parties, but copious amounts of working capital can make previously imponderable operations possible. A popular support network or false front organization to raise donations provides many of the benefits, but requires a visible channel to present a public face. Criminal activity to raise the necessary funds provides any volume of capital, while necessitating only the same skillset and tradecraft, one of the many reasons why OpFor and criminal enterprises on a global scale are finding common ground.

Armament for OpFor varies with the intent; DOS-M attacks might require plastique, DOS-V attacks need computer hardware and software, psywar attacks rely on domain specific knowledge/intelligence and access, polwar needs opportunity and the ability to react more than anything else. Beyond 'rightsizing' the attack and proper selection of the armament, IWAR is very much about denial–collapse or contamination of some element of the infra/infostructure, either under 'normal' circumstance or perversely at a time of special need of it (sabotage of a fire control system may not be noticed until the fire starts). Conventional weapons (and I'm freely lumping information warfare attacks here) are effective when used in the right place at the right time; weapons of mass destruction (WMDs), on the other hand, are also inherently about denial. For OpFor, WMDs are cognitive overpressure: nuclear weapons devastate everything, including everything worth having; chemical weapons are, oddly enough, more acceptable, under the mistaken belief that they are 'more controllable' in their usage, but still wildly indiscriminate; and biological weapons, well, biological weapons should scare everyone silly, since Mankind is fighting a potentially losing battle against them already. What makes the topic of WMDs interesting in an IWAR context is not what IWAR OpFor can destroy, but what they can restore–nuclear imbalance. Nuclear weapons have long been locked away from battlefield or political use by their threat value–Mutually Assured Destruction, deterrent value, trigger deterrents, and so forth. Command and

control of these weapons systems, however, reflect the period they came from, the Dark Ages of modern computing–authorization codes at rest or in motion can be scrambled or destroyed, and without them, older command-and-control organizations won't use the weapons, and more recent models are essentially inert without them. Nations who have not yet joined the Nuclear Club, but find their actions circumscribed by the lack of parity, can act in their own benefit to restore it–not by gaining their own weapons, but through denying them to the greater powers. This possibility alone could make Cornwallis's surrender of British forces at Yorktown while playing 'The World Turned Upside Down' sweet nostalgia.

Intelligence, not only the cognitive sort, but the gathered and analyzed sort, is the lifeblood of an IWAR OpFor; setting an intelligence objective and seeking to understand the target (and the 'Wirkung Im Ziel' or 'effect in target' you want to induce) are achieved not only by mapping dependency networks, but by more common forms of espionage. The sort of data necessary may be factual data (political, industrial, economic, technological, personal) or behavioral, but the act of gathering the data shouldn't trigger a Heisenberg effect, where the act of intelligence gathering effects the target. This usually means that passive, rather than active measures will be taken–technical intelligence, signal intelligence, etc. rather than human intelligence (which does have a greater tendency to tip the hand of the observer/OpFor). The special case of 'net-based open source intelligence' (NOSI) should be discussed, particularly in light of the recent attention it has been receiving in the political, business, and intelligence community. I personally have great difficulty in understanding why it is receiving the sudden attention, or why anyone seems to think it anything new. NOSI is what I refer to in my own work as 'research'–and that is not to say that it can't be a powerful tool; after all, Reagan's NSDD 144 and 145 were specifically targeted at the fact that individuals in the public domain could aggregate various bits of unclassified data, and with a little educated guesswork, derive classified data. The case of James F. Dunnigan's "Strategy & Tactics" magazine is a case in point–the subscriber list read like a "who's who" of military and intelligence, because the comparative statistics he generated from public data on, for instance, NATO versus Warsaw Pact weapons systems were better than what each organization was generating and using internally. NOSI is, however, only a subfunction of intelligence and espionage, and the part can't replace the whole; NOSI is the selective subset derived from the community memory or infosphere, an agglomeration from what we collectively know in public, where members of the intelligence community are trained before they have access to more restricted but presumably more detailed and specific information. It is naive to think that NOSI could replace the espionage function against a closed society or OpFor; in fact, NOSI works best for OpFor as an OpFor asset, or when turned against developed Western societies. In short, NOSI favors the attacker, but it, like IWAR itself, is nothing new.

As discussed earlier, dependency networks or infra/infostructure maps are generated from this sort of intelligence; whether from research or espionage, they work on 'soft' and 'hard' targets (in fact, such network diagrams quickly demonstrate the fallacy of 'isolated systems' or 'minimally sufficient infrastructure'), and allow OpFor to map the consequences of their tactical moves as they work to accomplish their strategic objective. A look at some of the potentials, and the probable OpFor specifics, will hopefully engage the reader.

IWAR POTENTIAL SCENARIOS

This is much more a book of ideas than a book of rules.–Erskine

State vs. State conflict will certainly be possible, however improbable it seems from some factors (notably a State's restricted viewpoint of politics and warfare, organizational difficulties, etc.); the sheer audacity of the move, combined with certain definite benefits the aggressor would gain, precludes me from ruling it out. In fact, I can imagine and speculate freely.

An IWAR capability solves a number of problems most nations have with establishing and asserting their powerbase (more on this shortly); in fact, if the goal is military and political effectiveness, and not tanks and troops marching on parade, IWAR confers the benefit that it favors the 'weak.' As the United States discovered, much to its chagrin, in Viet Nam: primitive infrastructures can be horribly robust, essentially requiring the wholesale slaughter of every man, woman, and child to achieve victory; while their more advanced infrastructures can be destroyed, damaged, impaired, or finessed with considerable ease. Not that the United States hasn't learned this lesson, as Desert Storm's massive destruction of Iraqi infrastructure demonstrates; whether they will ever have quite such perfect circumstances again remains to be seen.

States with the intent and will are most likely to build offensive capacity of some sort of another; more advanced nations, the United States among them, are rapidly becoming worried regarding their own vulnerability and are attempting to foster 'crash programs' to establish defensive strategies, tactics, and processes. While the idea of a 'Pearl Harbor' style attack is possible, the efforts undertaken as of this writing are humorously inadequate and misguided; their mispreparation merely increases the probability of occurrence and success. Other powers, peripheral or neutral, would find benefit in having an IWAR capability as a 'poison pill' (willing internal destruction of the infrastructure and infostructure in the event or threat of invasion, for instance) or for the deterrence and trigger deterrence value (retributive IWAR attacks upon an aggressor State, or waging IWAR throughout a region as a threat to neighbors to defend it in the event of an attack, or not to ally themselves with the attacker). The special case of IWAR targeting upon the nuclear command and control structure of another State (prior or subsequent to the commencement of hostilities) has been discussed earlier.

From an OpFor perspective, State origin or support does solve a number of operational issues: recruiting will come primarily from State assets (still with potential need of indigenous support); organization is likely to be a hierarchical command structure (with all the attendant problems of such); funding will be provided out of some State mechanism; armaments, at least of the conventional sort, and requisite training are a standard part of State resource. Intelligence is a questionable issue–most State intelligence organizations are poorly qualified to move into IWAR. Although the intelligence tasking that works for special operations or industrial espionage are useful and could be converted, such assets are not automatically or immediately capable of IWAR operation. The difference is the method of IWAR operations, not something that has, until recently, been a focus of the intelligence or military community, except for anti- or counter-terror/guerrilla groups. DOS-M is the most ready capability; the training and tradecraft are well within the special operations rubric, although the intelligence and target selection mechanisms are quite different. DOS-V capabilities are fairly new to States, being the domain of the hacker or criminal underground; State recruiting or acceptance of this set of techniques and personnel (the "it takes a thief to catch a thief" mentality) is quite low, and thus this is likely to be an on-going area where States lag behind the opposition for some time to come. PsyWar is within State capabilities–after all, they commonly have access to similar or identical processes and process models, or can obtain them–but the mindset, skill, and tradecraft are again lacking. PolWar, in particular propaganda/disinformation and agitation of various sorts, is already a common component of the intelligence capability of the States; the effectiveness of State-sponsored polwar, as opposed to independent polwar efforts, is an arguable matter; whether because the State-sponsored polwar efforts are 'heavy handed' and thus obvious, or that they are not managed by local, knowledgeable assets, modern State polwar efforts seem flawed.

1st-tier States are those whom I believe have the will as well as the most to gain, and among them include (no particular order):

CHINA-TAIWAN-JAPAN-RUSSIA-KOREA-SINGAPORE

China would benefit from any weakening in the region; specific attacks, for instance upon Taiwan, would be useful to 'soften' them up prior to an effort to reintegrate the province. Taiwan would certainly be less financially attractive if they executed some sort of poison pill strategy, but I suspect it would do them little good, and certainly not hold off an invasion; their IWAR interest should orient around defensive strategies, as counter-attack and deterrence will also be less than helpful (China has a strong history and policy of minimization of its dependencies). Japan, as a technological, financial, and industrial power is actually even more vulnerable than the United States–minimal internal resources, power dependencies, and the massive internal dependencies in the corporate zaibatsu with just-in-time manufacturing make Japan a house of cards; defensive planning should be essential, while their potential for offense action is questionable (defensive wildcard: the global consequence if Japan is attacked; offensive wildcard: the global consequence if Japan is attacked). Russia is already so inefficient, it is hard to imagine how it could degrade further; the 'long game' view of the adversary, however, coupled with the intelligence resources from the Soviet era, could make them a powerhouse in offense, if they only had a target (let the West take notice and beware). Korea (in particular the North/South split) and Singapore are both in similar situations to Japan; South Korea has much to worry about if North Korea begins to utilize its offensive capacity (note the defensive wildcard here is the same as with Japan). Of these States, China and Russia possess the greatest internal security from attack, and also possess the greatest likelihood to benefit from offensive capacity; on a conceptual basis, the Chinese have a long history of IWAR-like situations to study and learn from, while the Russians have the cognitive resources to help them bootstrap their own efforts.

ISRAEL/PALESTINE-IRAN-IRAQ-SYRIA-EGYPT

As horrible as it is to lump these together, the Middle East as a region will continue to be dominated by the actions surrounding these States. Israel has the most to lose if attacked with IWAR methods–hydraulic despotism, a fragile economy, potential loss of their covert nuclear capacity; if history has shown anything, however, it is that the Israelis don't mind cutting the ethical corners necessary to have their way, and that includes deterrent strategies in the region and against Western powers. The Palestinians have been living without an infrastructure for decades now, gaining a profound appreciation of ground; they have been quick students of history and their opponent, and could develop a wide array of strategies and capacity. Iran is likely to become the 'superpower' of the region, for what that is worth; if sanctions do nothing else, they teach you where your dependencies are, and the Iranians have also shown considerable savvy in the Middle East, Bosnia, and in the way they manage their global relationships; beyond a doubt, they would benefit from an offensive capacity, as well as the many flavors of deterrent IWAR strategies. In Iraq, very little else can go wrong; its infrastructure is already devastated, with little hope of repair because of sanctions; IWAR for revenge might look attractive, but it is worth noting that their attempts to promote terrorist attacks against the Coalition forces during Desert Storm came to naught (although Abu Iyad, who managed to stifle most of the actions, was later killed for it, and wouldn't be available to do so again). Syria has long enjoyed a position as puppet master in the region; it already practices IWAR in many forms, and will likely expand its capacity. Egypt rests its key position in the region on its possession of conventional military capacity; as we see how little that is worth in an IWAR context, it is unlikely to be able to make the shift, and will probably suffer the consequences. Offensive capacity then favors Israel, the Palestinians, Iran, and Syria; the entire region, however, could go up in flames (literally) with reprisal attacks upon the frail petroleum or potable water systems.

INDIA-PAKISTAN

I could have added this conflict into either Asia or the Middle East, but there are some critical differences; India has a varied economic structure, primitive enough to gain some robustness from that fact alone, yet at the high-end has technical resources along nuclear lines as well as informational, and has some history with Russia that could act in its benefit. Pakistan has similar strengths, as well as having been the staging area for forces into Afghanistan (and gaining in aid, training, and materiel because of that), and having had the funny little organization known as BCCI acting on its behalf for many years (the relevance of that will be clear later, when I discuss financial IWAR). That both States would be willing to go to war to destroy the other I have no doubt; subtle IWAR strategies would quickly degenerate into more conventional conflict or use of WMDs. The best hope for stability in the region is that some sort of Mutually Assured Destruction protection will continue as both build their IWAR offense and defense capacity; the effects to the global system, however, could be catastrophic, even if they don't resort to deterrence and retributive strategies.

UNITED STATES

The love-hate relationship that the world has with the United States does it no good in a world of IWAR; America is vulnerable in ways that few others can be–while Japan might be more fragile, an OpFor would have to be recruited from local assets, otherwise risk standing out; the United States has porous borders and little hope to track a foreign OpFor given the long history as 'melting pot' to the world. Intelligence and building dependency nets on potential U.S. targets is essentially a trivial matter (as you will see later as I discuss New York City as a potential target). The resources for any IWAR operational method can be obtained locally; recruiting is more a case of beating off potential members with a blunt instrument; organization and coordination can rely on the convenience of the U.S. communication infrastructure, probably the best in the world; funding is a trifling matter, obtainable from a large selection of criminal enterprises, or heaven forbid, profit from some front commercial venture. Most of the offensive strategies don't make sense in the context of a U.S. aggressor, unless you thought of them in the "do unto others as they would do unto you" context. I'm afraid that my assessment of the U.S. is as an 'accident waiting to happen.'

2nd-tier States are those whom I believe will build a capacity if for no other reason that to have it, and may find a purpose yet:

UK-IRELAND, FRANCE, GERMANY

These European powers have a long, colourful history as belligerents and allies; the potential for a Greater European War is never completely gone. The UK is still struggling to cope with the feelings of having once been a true Empire, and now being the lessor guest at a grand table; its relationship with Ireland reflects this. The long history of the British Empire is striking, particularly when you consider the rather shabby shape they left most of the world–Africa, the Middle East, India-Pakistan, China. The internal sickness of the UK probably prevents it from regaining any of its former glory; IWAR isn't the sort of thing that could give it to them either. They do need to have some concerns regarding potential attacks upon the UK, in particular from the Ireland situation; their complete lack of comprehension of the IWAR strategies being waged against them strikes me as something regarding which I should feel either rueful or embarrassed for them. France appears schizophrenic–on one hand, they assert their powerbase with nuclear weapons and expeditionary forces, and on the other they manage to let Algeria blow up in their face again. On the intelligence front, however, France accounts well for itself, including in industrial espionage; as much of this capacity could well be converted to IWAR capabilities, I feel certain they will have an offensive and defensive capacity. The French may also find the poison pill and deterrence strategies worth investing in, given the history of the region. The Germans have also had an active economic and industrial espionage capacity which could be converted to IWAR purposes; more

importantly for Germany is their financial strength in the global economy, and the potential power it could bring them. Germans take to war the way ducks take to water, so an offensive and defensive IWAR capability, if only for completeness sake, is probable–and may be useful if they find a need for military effectiveness without evoking suspicions of a German resurgence if they resorted to conventional military forces. I see France and Germany as potentials–France if only to assert what it feels is its prerogative, and Germany if only because it can.

SWITZERLAND, SWEDEN, BENELUX (BELGIUM-NETHERLANDS-LUXEMBOURG)

These traditional neutrals (or 'want to be' neutrals) have relied on tradition to keep their neutrality–as well as their 'poison pill' and deterrence strategies, not to mention their financial strength. An IWAR capacity would extend their existing posture, and also provide them with some interesting options given their already considerable finance orientation (see further below on financial IWAR). I see no reason to 'rank' any of these States, as they will build their own capacity for their own purpose, and tend not to be in 'competitive' situations.

STATE POWER--SOME ESSENTIAL BACKGROUND

> *"History knows many more enterprises ruined by want and disorder than by the efforts of their enemies; and I have witnessed how all the enterprises which were embarked on in my day were lacking for that reason alone."-- Richelieu, _Testament Politique_*

IWAR and the rise and fall of State powers runs like a thread through history, and if history is any teacher, IWAR is very old indeed; it is worth attempting to understand the nature of State powers and their origin, process, and decay, if for no other reason than the parallels which can be drawn to the modern States and organizations.

The historical tendencies (history is, after all, an inexact domain) appear to be that States rise on their industrial might and productive capacity; this economic power may potentially translate into military power for a time; eventually, productive capacity 'peaks' with saturated domestic and foreign markets; the invested capital into the installed base (resistant to costly retooling or technological innovation) combines with coalitions attempting to gain privilege, eroding the productive capacity; the economy converts to one concerned with 'financial engineering,' becomes introspective, non-creating, service-oriented, a net borrower rather than lender; an economic 'bubble' or conflict impacts on the already fragile political economy, and the debt burden slams home, as the productive and tax base is unable to do everything at once–maintain the economy, invest in new and risky potentials (whether new markets or new technology), service debt, and maintain social and military burdens. If this sounds familiar, it should–Britain, France, Germany, Spain, Russia, among others have all experienced the same pattern within reasonable variation, and potentially the United States and Japan are experiencing it at the time of the writing of this paper. One of the 'classic' warning signs is the mass-scale investment in armaments (purchased on debt or out of the tax base); this investment denies capital to other, more generally productive potions of the economy, and soon serves no purpose as swift obsolescence overtakes the invested-in generation of technology (complicated by the losses inside the tax base or even the loss of the tax base itself in the struggling economy).

Power is thus a dynamic state, coming from economic and technological advances, which with a combination of fortuitous social structure and geographic position, creates the powerful circumstance for influence. Just as in warfare, it isn't so much a case of doing things right, but doing fewer things wrong.

The advances that create the opportunity are almost always identical–production, technology, transportation, weaponry, and communication–as these serve the dual use of providing the infrastructure necessary for both war and trade. A case could be made, based on the historical evidence, that the 'wave' of advance, and thus of power, travels westward around the globe; no surprise, it seems to be the direction of exploration of the dominant power of the day, who invests in the region, and sets the 'floor' of technology in the region at the approximate level of its own domestic 'ceiling'. There is no place for the new territory to go but 'up'–and west. A study of the historical timeline pulls you from Asia to Islam, through Europe, eventually to the New World and the United States; from there I can only speculate, but a few key indicators are the industrialization and power consumption per capita growth rates, as well as investment patterns into infrastructure.

State power is a relative thing, and throughout history one State has risen and eclipsed others; the overshadowed States share some notable trends:

– Hierarchical control and centralized power structures, as for instance in the Ming and Islamic advances and then descent, is a crippling or fatal flaw when the leadership is incompetent, which appears inevitable. Predictable economic conditions, such as Europe and then the United States enjoyed, allow stable systems for investment and risk management. Having no unified authority that could stifle development, and freedom in technology, trade, and finances were and are critical to power.

– With the introduction of coalitions, fighting a sustained war led to the practices, far from over, of deficit spending, and the orientation of military status being equated to capital resources, cashflow, the interest rates and rating; the end result, of course, was and are loan defaults, currency debasements, property sales to afford to pay for military operations (which translate into lost income), property seizures, and taxes of every shape and form. Financial collapse is still the leading agency for peace, across centuries of conflict, from the Habsburgs to now. No matter how prosperous the times or the States, there are always gaps between their income and their expenditures.

– Gunpowder Empires are a horrible thing for everyone; both Japan and Russia experienced a power that used its monopoly on force, through the mechanism of being the only one with possession of firearms, to unify their respective domains. Of course, once the goal is accomplished through such means, the monopoly holder must stifle any other advance–trade, communication, technology, etc. could all threaten the monopoly, and so progress comes to a grinding halt. How is this troublesome? It creates creeping vulnerabilities–just as when Commodore Perry's "Black Ships" opened Japan in 1853, the 'outside' world will surprise you. The United States already finds itself a troubled power as well as a gunpowder empire since the collapse of the Soviet Empire; given the dire consequences of previous collapses of global powers and gunpowder empires, the potential breakdown of the U.S. could be a spectacular disaster. The U.S. vulnerability to IWAR, and the recent hysterical reaction to the potential threat, are merely symptoms of the greater problem.

As I stated previously, power and authority have devolved from the States; IWAR action at the State level will certainly be seen, but the 'real action' in IWAR is the non-State actors, who have benefitted most from the lost State prerogative of waging war or engaging in conflict, and in fact seem to be acting as the next mechanism to eclipse State power.

IWAR ADVERSARY--NON-STATE ACTORS

The capabilities of waging IWAR are very different from those required to wage more conventional war; there is no need for fighter jets, aircraft carriers, tanks, and legions of men. Once the materiel limitations are overcome, the singular difference rests with intent/will; I consider it a 'proof by demonstration' that, as many conflicts are currently occurring using the various IWAR operational methods, this limitation is no longer one. The methods of IWAR are well within an independent grasp:

DOS-M requires ordnance that is available in a variety of ways, from the black market, theft from State stocks, or even legal purchase (not to mention that the user may very well be the manufacturer); DOS-V technology and tradecraft has its origins in the private sector, with a considerable network in place to exchange the latest advances or refinements; psywar depends on domain knowledge of processes and process models which have their origin in the private sector; polwar has long been a capability of the free market–after all, the populations regularly overthrow and install new political leaders (even if the mechanism is an election). Other OpFor requirements–recruiting, organization, funding, armament, intelligence–are within the grasp of the lowest plebeian and, as discussed previously, certainly obtainable.

CORPORATIONS

Corporations, in particular the Stateless transnationals, have all the requirements for managing an OpFor to wage IWAR (State-supported corporations should be viewed as a variety of State-sponsored OpFor); targets could be anywhere across the scale and have been. Corporations have acted to overthrow States before, and have a distinct motivation to want an offensive and defensive IWAR capacity in dealing with other corporate or organizational threats; DOS-M attacks on opponent dependencies, DOS-V attacks for espionage or sabotage purposes, PsyWar attacks to undermine competitors, and PolWar to gain influence or privilege have all been used. Historical actions that have come to light by such organizations like ITT, Hughes and other defense contractors, the various petroleum and financial corporations, etc. are all good examples. Corporate intelligence and operational groups are at the forefront of offensive IWAR.

TERROR, GUERRILLA GROUPS

There is a blurry line that separates terrorism from guerrilla actions, and it has become popular recently to lump 'conventional' terrorism and guerrilla warfare in with IWAR. I hope the reader is following my argument well enough to recognize the differences, but it is worth pointing a significant one out–dependency. IWAR actions of the DOS-M sort could very well look like terror or guerrilla attacks–differences would be of intent and targeting. A bomb in a crowded shopping plaza is certainly a terrorist act; it could only be categorized as a DOS-M attack if it were intended to have impact on some sort of dependency (such as the financial impact from the destruction, closure, and reduced retail activity). I know it may seem like quibbling or semantics to some readers, in particular those who 'criminalize' such actions as a blanket policy, but one man's terrorist is another's freedom fighter, and those who have been terrorists in the past have gone on to be Presidents or win the Nobel Peace Prize. Once again, if the issue is effectiveness, and the OpFor has settled on DOS-M as an acceptable operational method, then such IWAR actions should at least be categorizeable in some fashion. IWAR terror and guerrilla actions have occurred in Russia, UK-Ireland, Germany, the Middle East, and the Americas; particularly interesting were Red Army attacks post-German Reunification, Abu Nidal and the assassinations of Sadat or Abu Iyad, and the links between guerrilla/terrorist violence in Central and South America for the drug cartels. The World Trade Center bombing in the United States is one that I personally don't classify as IWAR related; the conspiracy to attack New York City's bridges and tunnels, however, I do classify as an IWAR attack. My personal belief as to why the line is blurring between IWAR and non-IWAR guerrilla/terror actions is that more and more of the groups are becoming IWAR enabled, just part of their continual progression.

PARAMILITARY

Civil militia groups in places like the United States are clearly preparing for and executing DOS-M and polwar attacks; while the cases of the United States' claims that the Oklahoma City or Olympic Park bombings were militia action have yet to be proven, the militia training materials and activity clearly reflects an attitude supporting the assertion. Polwar attacks, in particular the net-based propaganda, are on-going; the traffic regarding TWA flight 800 in particular has clearly been a great mass of disinformation (which, incidentally, can be viewed as having contributed to the panic-borne

reaction in airport security and restrictive legislation). Various hate groups (with racial motivation) have taken to the Internet, throughout much of the world: neo-Nazis in the United States and Germany have coordinated uprisings and demonstrations, distributed propaganda, etc. In the latter case, the Wiesenthal Center fed the hysteria for their own purposes, among which was an effort to impose controls on freedom of speech. Fascism is alive and well, in all its forms, on the Internet.

CIVIL DISOBEDIENCE

The use of the Internet as a tool for civil disobedience (mostly peaceful) was natural; after all, it provides a communication mechanism that doesn't require State permission. In the United States there are examples of labor unrest, protest marches (affinity has either been regional, such as in California's reactions to various legislation; issue, as in 'issue' riots in Florida; racial, as in actions against Texaco), and an interesting demonstration of power by the Nation of Islam with the Million Man March. French protests have made extensive use of electronic coordination, and there have additionally been DOS-V attacks associated with the same protests. Polwar tactics are steadily being incorporated into the standard political process; in a few years, it may be necessary to stop drawing a distinction, as the political process will have degraded to such a point where there is no discernable difference.

POLITICAL

I'm making a distinction here, as 'political' action by groups is waged either against States, or by various other means. In the U.S. elections of 1996, however, there were a few interesting cases of mailing lists belonging to candidates' campaigns being destroyed (whether by a DOS-V attack of by a 'double' inside the organizations is unclear), web sites being hacked, and the curious case from the previous Congressional election of the polwar techniques being used against the re-election of the Democratic Speaker of the House of Representatives. The history of politics is filled with these sorts of 'dips' into dirty tricks and generally loathsome strategies and tactics; whether the political process is experiencing a temporary period of such behavior again, or if this is actually a significant and permanent change remains to be seen.

IDEOLOGY

Just as the first transnational wars were fought over a transnational issue (the Reformation), modern ideological differences are iwarred about globally; witness the various actions of Greenpeace, Animals Rights activists, and in the United States the Pro-Life actions. Environmentalists have shown little reluctance except for the loss of human life, and have waged IWAR in all its forms; Animal Rights activists have stuck to DOS-M and polwar sorts of attacks; anti-abortion violence has been mixed, some attacks for personal reasons, others clearly to discourage others from working at or using the services. Recently all these sorts of groups have begun to show an increasing level of technical and tactical sophistication, a trend that is likely to continue.

CRIMINAL ENTERPRISES

Willie Sutton was once asked why he robbed banks, and his response was that was where the money was; modern criminal organizations have taken note that in the modern world, the money is with technology, and so are other benefits. The drug cartels are extremely technologically sophisticated, and have used DOS-M attacks not only to discourage prosecution but to settle disagreements with other criminal enterprises by assassination of critical personnel (chemists); DOS-V and PsyWar attacks, in particular against law enforcement agencies for the purpose of gaining information or causing damage have occurred; PolWar efforts vary from the purchase of political influence to supporting either side of the drug legalization issue (where a difference of opinion on the impact of legalization to cashflow causes the bifurcation). Money laundering relies heavily on today's electronic global markets, but hasn't peaked yet the way it will with true electronic cash. Industrial espionage is a multi-billion dollar (U.S.) industry, ranging mostly from sabotage with DOS-M/V attacks and intelligence efforts; the 'dirty little

secret' of global business is gaining in strength–as more information, the more valuable 'process' information in particular, enters the digital world, it becomes susceptible.

HACKERS

The hacker underground has been the origin of the tactics (but not the strategies) of DOS-V; the vulnerabilities of the global infostructure can be seen in even the most rudimentary attacks, such as SYN floods, web-page hacks, system cracking, etc. As annoying as such attacks might be, however, I refuse to criminalize the hacker underground as many have done–given what they have to work with in the way of technology and knowledge, if they truly wanted to cause damage, they could and would have. Attacks on hackers, crackers, cyberpunks, cypherpunks, etc. are specious in the extreme.

FINANCIAL

The topic of financial IWAR is too important to cover briefly, and so I have outlined later in this paper a special case study.

INDIVIDUAL

There is much to recommend the 'conspiracy of one'–nothing about IWAR requires manpower that one individual can't make up for in time and dedication as opposed to cooperation. OpFor recruiting, organization, and probably funding become non-issues; operational methods lose little of their effectiveness, as the issue is one of leverage through taking advantage of dependency; intelligence is the only burdensome issue, but not one that is insurmountable. The benefits, particularly in security, are considerable. IWAR could very well be the ultimate empowerment of the individual.

IWAR TARGET--STATE

IWAR operations against the State are complicated, as the State has many dependencies; on the other hand, time is on the side of the attacker, and OpFor always knows where to find the target. IWAR attacks can be made on those functions that have become exclusive to the State, namely military (which is how you define guerrilla actions–they only target the military or political infrastructure), management (administrative, legislative, judicial), or monetary power. None of these State components is an easy target: military targets have a tendency to shoot back, political targets have a way of becoming martyrs, and monetary attacks require resources (see the financial IWAR case study below). IWAR can take the appropriate step of moving one layer of abstraction from the State to attacks on the economy or infra/infostructure, as discussed previously. The idea of attacks on people is one that merits special attention; in primitive social structures, the people actually are the infrastructure, and so IWAR attacks are difficult to distinguish from mass violence; but in advanced cultures, most of the population actually has very little to do with the main infrastructure (except in peripheral ways), and attacks on people are pointless from an IWAR perspective. This distinction is critical–IWAR can, in many ways, be a bloodless but effective form of warfare. Wars in more recent history however, and the after-effects of such conflicts, have commonly been upon civilian populations: Jews, Gypsies, Palestinians, Vietnamese, Iraqis, various tribal violence, etc. If war and conflict are moral in any sense of the word, perhaps IWAR could make it more ethical.

IWAR TARGET PROFILE: NEW YORK CITY, UNITED STATES OF AMERICA

I thought the reader would, perhaps, find the exercise of looking at a target and working out potential areas for IWAR attacks intriguing; the ethical dilemma such an exercise poses will be dealt with by being expeditious and brief, but to provide a conceptual guide for the reader to set off on his or her own speculation.

My process, to establish a sort of handicap to offset my professional experience, was to set a few deliberate constraints: only an hour of research, and only using NOSI (where I used three 'launch' sites– Alta Vista, Yahoo!, and the SEC-EDGAR indexes and databases). As I have said before, NOSI favors the attacker, and indeed, the sky is raining soup, so grab a bucket. Note that the categories used are rough generalizations derived from building dependency networks on previous occasions.

Communications: Conventional communications information, including service maps and other information on the network was available from both long- and short- line providers; the cellular system provided details on cell specifics, including maps; technical information on communications systems, including failures or attacks, were available from both public and 'underground' resources. Physical details needed to start research for DOS-M attacks were available, but the richest materials here were for DOS-V attacks and psywar, including detailed information on things like the 911 (emergency switching to law enforcement) network.

Media: Certainly not shy, these organizations (radio, tv, newspapers, magazines, publishers) provide everything from photographs of their staff and locations, information on their facilities and tours, as well as acting as a further information source on local events and conditions. A wonderful resource for DOS-M attacks, and their ready presence on the net reflects an ability to use these outlets as the crossover point for polwar propaganda and disinformation operations into the mainstream media.

Power: Maps and equipment details were available, as well as details on emergency preparation, how they handled previous emergencies; financial reports disclosed considerable detail, as did their utility reports, as well as pointers to fault analysis reports on the system. Other information, not New York City specific, on loss of service (including DOS-M attacks) in the power grid would be particularly helpful in planning and execution.

Water: The city provides considerable data on its water system, problems they have had with the system, and maps, etc. Other academic sites had a number of studies on water contamination, including details on which microbials were not controlled by the water decontamination systems.

Fuel: New York City has a considerable infrastructure of fuel oil, petroleum, and gasoline. Information on refineries and storage facilities is available in the financial reports of the various suppliers. The public nature of these facilities makes them an element of the infrastructure that almost can't be protected from DOS-M attacks.

Banks: As a financial capital of the world markets, banks in New York City are prominent and proud, including the Federal Reserve, which provides considerable data on itself, its function, and personnel. Other banks are just as open, including site addresses, maps, architectural diagrams or photos, etc.; a few offered location information on their Automated Tellers, which I interpret as being located in points of convenience or great traffic, and so of particular interest from a DOS-M perspective. While electronic banking is just beginning, the DOS-V potential is extremely high.

Markets/Exchanges: The New York Stock Exchange, NASDAQ, broker/traders, etc. provide detailed information, and the wealth of market related information reflects the significance of this section of the infra/infostructure as critical, but inside my self-imposed limitations, I was unable to dedicate the time necessary. Needless to say, DOS-M attacks have been successful in the past, DOS-V attacks are quite possible; financial IWAR is covered in detail later in this paper.

Air Travel: Information on airports, airlines, schedules, etc. is available, including access to the scheduling systems, of interest for DOS-V attacks. For DOS-M attacks, there are maps, information on security warnings and details, etc. Recent media stories on 'penetration' tests they've run (making their way into baggage handling, cleaning services, the cockpit, etc.) have provided helpful OpFor 'dry-runs.'

Rail: Railsystem maps, schedules, peak times, and other details are available; of interest were the numerous details available on train derailment (whether by accident or intent). Cargo lines in New York State on occasion were labeled as carrying hazardous materials. Rail is not only the best option for OpFor travel, but as a soft target.

Public Transport: Public systems such as subways and buses made available bus and train route maps, schedules, and peak traffic data; reports regarding recent attacks on the subway system (including a firebomb attack in NYC, and the sarin gas attack in Japan) were potentially useful for the offensive and defensive detail they provided.

Bridges/Tunnels: Bridge and tunnel information was particularly useful–not only maps and traffic data (including peak loads), but structural information, including data that came out at the time of the conspiracy to attack a number of such sites. The bungee and base-jumping subcultures also had detailed information on bridge security, structure, and height (making possible, for instance, driving an explosive-laden truck onto a bridge and then safely jumping off).

Schools: Educational facilities from day care through university level make considerable information available which would be useful in DOS-M attacks looking for casualties (from Board of Education photos, staff photos, student headcount, facility maps, event schedules) to other sorts of attacks (budgets, etc.).

Religious: Both churches and synagogues made information available on location (including photos), layout, membership, and events. Information on a recent set of arsons against religious institutions disclosed considerable detail on the functioning of such organizations, as well as highlighting their vulnerability.

Administrative: City administration provides not only budgets, but considerable other financial detail (useful in any number of attack methods) for bonds and for various credit mechanisms.

EMS: Information regarding police, fire, ambulance, and other emergency service detailed past performance, zones of coverage, resources in equipment and manpower, police doctrine, command hierarchies including photographs and biographical details, and even the communication frequencies (and codes) used for tactical control.

Business: Businesses certainly love the net, and many of the essential infrastructural elements were represented, including food (grocers, markets), medical (hospitals, physicians, clinics, nursing homes, labs), retail shopping (one would get the impression that New York City spent all its time shopping based on the detail of maps and data). Modeling of the economy and sections of the infrastructure has already been performed.

Public Events: From small to massive scale events, whether entertainment or sports, detailed information is available (including, as usual, maps and layouts); tourist oriented information provides a wealth of additional data, from hotels, tourist areas, tours, maps, and schedules.

Government: Represented are any number of local, New York State, Federal, and international (UN, embassies and consulates) sites and personnel, so many in fact that it was impossible to even sort while allowing time for checking the other categories.

Infostructure: There are available a number of service providers and even network topology maps, details from the recent SYN flood attacks on local providers, and a wealth of underground material that was impossible to plumb the depth of.

General Amazement: Not only were maps available in general, there are a number of 'address finder' services where you can enter an address and it will show you where it is, in detail; there were also a

number of sites that would offer live video of the location or the surrounding area (so OpFor can take a look at where the site is on the address finder and figure out what they are watching, location surveillance via the net).

While I didn't use the tool for speed sake while looking for this information, an OpFor could shelter their identity while doing such research using the Anonymizer (http://www.anonymizer.com); this way if someone were to try backtailing, there is at least one level of indirection in place.

My general feeling during and after the search was that I could have blocked out fairly detailed operational plans using the information I had, even if I had never been in New York City before; to test this, I used another professional who has not been to the city and re-ran the exercise and discovered that I was correct (to check the result further, we switched places, where the other professional involved researched a city which I had no familiarity with, but performed equally as well regarding). We might have differed on selections of attack methodology against a selection of targets, but the fact remained that another professional felt it just as powerful a tool as I did; I hope the reader will let me know their opinion on the matter. As any casual user of the net will discover, New York City is not an atypical example of the sorts of information available.

It is worth noting a phenomenon the reader might not have observed: function forces form, the target selection as a 'physical' place makes the preponderance of attack related information orient around a DOS-M operational method. While the collateral effect of many DOS-M attacks on the target would have consequences related to the other operational methods, it can be rather startling how a cynosure upon a target causes a congruent focus and reduction of operational options. Regardless of such narrowing, OpFor gains considerably from the use of the net:

- Superior knowledge and intelligence, including dependency network maps;
- Improved target selection, varying the rules of engagement, increased leverage, and consequence prediction/management;
- Surprise and security, with small chance of surveillance 'tipping off' the target;
- Sanctuary (cover and conceal) for OpFor could easily have been located and obtained through the net, potentially with no need for human or later face-to-face contact;
- OpFor can be decentralized--coordinate dispersed, act concentrated;
- While this example does focus on 'ground,' there is no 'front' or 'rear,' there is 'local' control, and no OpFor 'centre';
- OpFor remains fluid, mobile, and dynamic;
- No time/space constraints or obstructions;
- After-operations psyops, including media 'spin control' can also be managed via the net;
- Beyond a doubt, this method is unconventional and unexpected.

IWAR OPERATIONAL METHODS

As I have discussed in this paper, and in some detail elsewhere (see my Infrastructural Warfare Threat Model), I categorize IWAR methods of operation against dependency networks and infra/infostructures as such:

- DOS-M: including some forms of conventional warfare (elements of attrition and clearly manoeuvre warfare), guerrilla warfare, terrorism, and various 'denial' attacks such as those using WMDs;

- DOS-V: variously termed infowar, netwar, cyberwar, etc. where the attacks have the same philosophy and intent, but vary as to the scale, from individual-oriented attacks to 'Pearl Harbor' mass scale attacks;
- PsyWar: attacks upon processes, process models, and decision models that don't aim to destroy, but to subvert; I have referred to this method of attack as a 'Hashishim approach' elsewhere;
- PolWar: technologically augmented political warfare, including propaganda and disinformation, agitation, and subversion directed specifically at the political process; or 'politics by other means,' but increasingly 'mainstream' politics itself.

The military, intelligence, law enforcement, political, or other professional reviewing this categorization should be able to find some aspect of their own experience which allows him or her to comprehend–this is nothing terribly new phenomenologically, merely a different conceptual spin in ordering and understanding (yes, and operating). As such, I feel no need to expound upon each individual operational method again, but I wish to walk through a consideration of an interesting hybrid that utilizes all the IWAR methods, and consequently opens up a previously unconsidered set of attacks which clearly have their provenance within the IWAR domain.

IWAR OPERATIONAL METHOD HYBRID: FINANCIAL IWAR

> *"...economic power will be the key to other kinds of power..."– Richard Nixon*

SOME ESSENTIAL KNOWLEDGE AND BACKGROUND

This truly appears to be a blindspot for most warriors, and I suspect it is because the domain knowledge requisite for exploration and understanding is generally not afforded, given the considerable other essential skillset warriors must maintain; a deficiency of financial knowledge doesn't hamper the career of the professional soldier, and around the world, soldiers don't seem generally to take finance seriously. A brief introduction or review is thus necessary, so bear with me.

Corporations and companies are the general tools for organization in the business world; functionally, they should be quite familiar to the professional–they have intent/goals, methods, organization, funding, materiel, intelligence (marketing), etc. Operating a business entails risks, only in business, companies have tools to hedge and speculate, to insure themselves against risk. The popularized Japanese dictum of "Business is war" is, consequently, one that I've always considered erroneous; while war is about risks, business has this added dimension of tools to manage risk (and IWAR upon business is the process of the removal of such risk hedges and subsequent 'pushing' in the right direction).

Companies need to manage risks–currency, interest rate, or financial fluctuations; in finance, risk is defined as the uncertainty that asset values, cash flows, or business objectives may be achieved or maintained. Once risk is quantified, a risk premium (the price of risk) can be offset in any number of ways. The most common method is to hedge through diversification, maintaining a number of varied operational or financial operations; since market moves that create risk are highly relative (what is good for one business is bad for another), hedges are themselves variable to offset relativistic shifts in values. Companies which are better at managing their risk are priced better in the market and have a cheaper 'cost' of money (debt), so numerous financial tools have evolved over the centuries; companies which are poor at managing their risk soon suffer Darwinian selection and cease (an idea which may have startling consequence in the context of inter-corporate or financial IWAR, or in the valuation of companies by markets).

The financial tools developed to manage risk–options, swaps, futures, derivatives, etc.–are interchangeable in many ways, and the global markets have therefore become linked; pressures on one sort of financial tool will quickly spread to impact on any of the interchangeable tools. Market links mean that the risks of shock to one market or tool quickly spreads to others; in fact, it is now realistically difficult to assess risks through these linkages because of the dynamic and rapid shifts of dependency relationships between the various markets and assorted tools.

HISTORY OF FINANCIAL MANIPULATION

From an IWAR perspective, attacks using financial dependency have a long and colourful history. Some notable occurrences:

- Thales of Miletus, the ancient Greek who invented the option, with which he 'optioned' olive presses, and controlled the market in olive oil; he paid small up-front fixed prices to secure the use of the presses at a later time, at which point he was then able, through his control of the market, to charge whatever fee he wished to the olive growers in need of the presses.
- Both the Dauphin and Henry the VIII, who profited themselves, for a time, through their debasement of currency, over which they had monopolist power; their actions led to Sir Thomas Gresham formulating Gresham's Law: "If two kinds of money in circulation have the same denominational value, but different intrinsic values, the money with the higher intrinsic value will be hoarded and eventually driven out of circulation by the money with lesser intrinsic value." In other words, Gresham noted that non-debased currency when received would be kept, while debased currency would immediately be spent, commonly for the settlement of public debts–bad money drives out good. Foreknowledge of government debasements even led to a specific practice of 'leading and lagging'–timing your payments and receipts to protect against and even profit from currency debasements. None of this seemed to impact on the later actions of John Law, or those of the French Crown, Banque Royal, and the Mississippi Company bubble; nor the centuries of continuing European trade wars waged through the devaluation of currency (making your exported products cheaper and more attractive to foreign markets, prompting others similarly to devalue in response) and tariffs.
- The generally syndicalistic behavior for centuries by the Japanese Zaibatsu/Keiretsu system, including the interesting actions by Mitsui to collapse their own government over the issue of the gold standard (and for which the Blood Brotherhood assassinated the Mitsui leaders).
- The use of arbitrage (profiting from a price/information inefficiencies by buying in one market and selling in another market to your benefit) in the early currency wars involving the Eurodollar and petrodollar.
- The 1979 attempt by the Hunt family to corner the silver market using futures contracts, a lesson in how hubris leads to nemesis.
- Inside the last decade, there are a few quite notable financial IWAR attacks. Regulation on the Nikkei drove trading onto the Singapore exchange at the same time that the Singapore International Monetary Exchange (SIMEX) was a battlefield against the yen; the Nikkei was being manipulated by ramping into thinly traded components of the index, and finally the Kingdom of Denmark issued Nikkei 'put warrants' which helped deliver the coup de grace to Japanese financial health (and from which, incidentally, they profited). The death of the Bretton Woods monetary agreement as well as the European Exchange Rate Mechanism, when in 1992/93 a number of hedge funds, international currency traders, and some of the first examples of financial iwarriors

(among them, George Soros and Stanley Druckenmiller, who did appear to functioning with specific intent) forced the States (among them Britain, Ireland, Italy, France, Sweden, and Spain) to float the exchange values of their currency, to their loss and the traders' profit. Also notable financial IWAR actions were the operations of the Bank Negara of Kuala Lumpur, Malaysia, where the central bank waged attacks in the currency markets (aided by their intelligence functions as well as cooperating banks which also profited in the attacks), using finance as a weapon (until brought low by overextension against the sterling).

FINANCE--THE LEADING EDGE

The financial community has, for centuries, been at the leading edge of almost every advance, conceptual and technological; certainly there are selfish reasons of profit, but the general effects in the infosphere (and in fact, a good case could be made that they are the primary supporters of the infosphere) of information transmission, analysis, even mapping of dependency networks have their origin or comparable process in the financial network.

A concept I've used on occasion in my work is that of community memory–the collective content or knowledge of a society; the Internet is a good example of a community memory. The net is an exchange tool for the wide array of communicable human thought and experience; almost anything I want to know, question I want answered, concept I want to explore, etc. I can discover. There are, obviously certain caveats–in particular, coping with accuracy and bias, where the concept of reputation capital (judging whatever entity that supplies the information) is of particular importance, but it still takes human judgment to gauge bias and correct for it (or not, in the case of affinity or 'intentional' groups).

While the net is a fledgling community memory, the financial markets are veterans. The economic principle of 'perfect information,' in particular how it relates to price, is telling: conceptually, it means that the price on anything will reflect the sum total of the market knowledge regarding the priced entity, or in short, price is formed/set by consensus (which, you should note, neatly encompasses the Law of Supply and Demand). Mathematical relationships exist that define the information value of pricing–efficiency, or the degree to which the price reflects all information which might effect the price; and volatility, the probability of a change in price over time (predicting potential information, new or changing, and efficiency). Having superior information, as reflected by 'inefficiencies' (and note here that market inefficiencies may also represent more than just flaws in information or the structure; for instance regulations, which unlike in information networks are not routed around, but taken advantage of) in the marketplace or community memory, may temporarily allow arbitrage, the exploitation of differences, but price rapidly becomes universal across markets and across interchangeable financial tools.

Money (a store of value, a medium of exchange, a regulator of economic activity) is a central function and monopoly of a State; recent events have shown, however, that State control, geographic, and legal barriers are fictions–there are no barriers to trade, no borders to money, no controls but the markets. Financial markets, however, are about perception, in particular, the perception of data such as money and price.

The world of the trader is the world of community memory (price) and dependencies (which can be arbitraged, leveraged, exchanged, hedged); the data passing through this infosphere is transformed to information, analyzed, and opinions drive pressure back and forth, microseconds through the aether. Data is viewed differently (Is an entity a sound investment, or overpriced? Is this risky? Will this product be a success?), otherwise there would be no fluctuation without new information. In fact, traders look at information in different ways: 'fundamentals' trade on basic economic data, supply and demand; 'techs' trade on graphs, price analysis, past price trends; 'quants' trade on the probability of moves based on arbitrage of market relationships; 'judgment' traders try to think like their opponent,

calculate the potential alternatives, and systematically cut them off. Even the difference between fundamentals and techs is striking–fundamentals look at the real world (data), while techs look at graphs and price (which is already one degree further in the value chain, data processed into information). In a world where data, models, and community memory are so critical, and approaches so different, a whole set of potential avenues of attack open up, and in ways that are not only not currently regulated, but would feed on regulatory or enforcement attempts.

FINANCIAL IWAR

Recently an American General commented that he wanted to learn about information warfare because he didn't want to "get his ass kicked by a hacker with long hair wearing a T-shirt." The man at the computer that the General truly has to be afraid of isn't necessarily a hacker, but a trader.

Imagine a transnational financial organization similar to the one I'm about to propose and you'll see what I mean; the world already saw something similar, Bank of Credit and Commerce International (BCCI), but while BCCI had many of the components, it didn't have the advanced technology, nor the intent (to be more exact, not this specific intent, but there were many similarities). Let me call this financial organization 'Hortalez & Co.' and name the proprietor as Pierre Augustin Caron de Beaumarchais; historians will recognize this as the organization used to launder funds from the French to the American Revolution against Britain. Hortalez is no short term operation, but a long term mechanism aiming to utterly destroy their target using every means at their disposal: no mercy, no forgiveness, no hypocrisy, but subtlety whenever possible. Among Hortalez's activities:

DESTROY THE TAX BASE

Given the State reliance on the tax base for its function, undermining this financial strength is crucial; offering 'electronic money' and flight capital services, including money laundering, puts considerable capital at Hortalez disposal, which will be useful in its larger plan. Hierarchies and monopolies are important targets–undermine currency values with counterfeiting, target the instabilities of other monopolistic controls, including intellectual property. Attacks affecting State dependents (such as welfare or other social 'safety nets') would be deferred, leaving the financial drain in place as long as possible, with subsequent attacks timed to trigger a more general social unrest.

ATTACK THE ECONOMY

This is the epiphany of 'deep battle'–hit the sectors that make an economy strong: financial organizations, industrial and agricultural production capacity, technological development, communications networks, transportation, and armaments. Initially this will be polwar and psywar attacks, but as situations decay, more overt attacks using DOS-M/V methods will come into play.

Given knowledge of dependency networks, financial relationships, and foreknowledge of attacks, Hortalez can profit from the global financial market reaction to these attacks. A critical dependency to track is the effect of products and commodities on currency values, the so-called 'currency of determination' relationship. Diversification efforts, particularly in sectors of the economy relying on critical materials, components, and products must also be undermined.

ATTACKS IN THE CURRENCY AND INTERBANK MARKETS

Markets are linked, so efforts in smaller, more readily controlled markets are preferable, and leverageable back out; the collateral effect in the interbank market, which moves more than $1 trillion dollars (U.S.) a day, will be immediately felt in banks, insurance companies, investment houses, and then through into the rest of the economy. DOS-M attacks from Hortalez's operations arm can target commodities, allowing exploitation of those futures markets; corporations can be attacked to deliberately profit off their instability as well as impact the dependency networks.

CORRUPT THE COMMUNITY MEMORY

'Perfect information' can be manipulated by impacting on the 'fundamentals' basic data, and financial manipulation coupled with psywar attacks on the 'quants' and 'techs.' Risks can be deliberately manipulated–altering volatility values, arbitraging the effects.

Hortalez could operate a public financial enterprise–banking, a hedge fund, etc.; this would provide the underlying financial pool necessary to exploit the other capabilities of the organization. The organization would also have an operation dedicated to DOS-V and psywar operations–perverting program trading models, undermining other organizations, destroying competition and targets. There would be a covert operations arm for DOS-M, similar to the BCCI 'black network,' but targeting denial attacks (for instance, on sensitive commodity production, manufacturing, or volatile sectors of economies) in line with the larger intent of the organization as well as for profit–the more money Hortalez has at its disposal, the greater a weapon it becomes. Also similar to BCCI, the organization would need a polwar arm to manage global propaganda and disinformation, not only on its own behalf, but against targets and political systems. Hortalez could start small–gaining resources as it grows, using money as a weapon, intelligence to make trades, and operations to make its investments pay off.

It is my belief that Hortalez is something that is beyond that ability of States to control or combat; regulation or legal action can merely be used to profit off through arbitrage; global markets mean that the target State would not necessarily have jurisdiction over any of Hortalez's actions; the slow, subtle course of action need never even be exposed. When BCCI tumbled and crashed, the pyramid scheme at the heart was the issue–Hortalez wouldn't need to be a Ponzi scheme, need never formally 'break' a financial law, or undertake any other criminal action in its target's territory. In the aftermath of BCCI, the black network has never been identified or put out of action; in all probability, an organization like Hortalez could weather any similar storm. This form of IWAR OpFor is alien to most professionals in the IWAR and related domains, and yet it frankly represents the perfect manifestation of the field.

DEFENSE-IN-DEPTH: BATTLING IWAR

> *If there is a Way involving the spirit of not being defeated, to help oneself and gain honour, it is the Way of strategy.– Shinmen Musashi*

Throughout this paper I have, on occasion, referred to the concept of 'defensive IWAR'–something of a misnomer, as IWAR is an offensive strategy, and defense is more a case of understanding the offensive mechanism and addressing it. Beyond a doubt, a defensive capacity implies an offensive one, but IWAR conflicts are not like a board game, conventional, or guerrilla warfare; there are no force-to-force conflicts, but more a case of withstanding the offensive attack while either attacking back, or tracking and neutralizing the offensive force. I'm going to assume the creation and maintenance of an offensive capacity as a given; without this requisite domain knowledge and expertise, the chances of recognizing and managing against an IWAR attack drop precipitously.

IWAR takes its strength from the opponent; as a structure becomes more complex, it has very little choice except to specialize and create dependencies and infrastructures. Modern social structures are intricate and convoluted networks of relationships, dynamic yet fragile. Just as an IWAR OpFor targets on dependency in all its forms, the primary focus of defensive IWAR strategies must also concern itself with dependency; IWAR is like water, changing form to fill any shape vessel, and capable of seeping in through the smallest of conceptual flaw.

DEPENDENCY

Dependency and associated risks must be managed; to effectively be managed requires mapping of the dependencies first. Individuals, organizations, and States should perform the 'day in the life' exercise to be aware of and understand their own function and the points of reliance on elements over which they may lose access, service, or control over. Diversification is essential, but not always possible; fortification against IWAR threats isn't the sort of thing that happens over-night, automatically, or even simply–there are just too many factors of dependence. The solution is not a 'point defense' or 'perimeter defense'–any hardened point or points can be worked around or obviated.

DEFENSE-IN-DEPTH

T. E. Lawrence, in World War I, commented that while his opponent could reinforce any point to withstand attack, he couldn't reinforce every point; IWAR, then as now, relies on this selfsame point, and more–there are very few organizations or entities that are self-reliant in toto. What is needed to address this is a fundamental difference in the design, implementation, and operation of the various elements depended upon in a society; as no one particular point can be made totally independent and secure, then every point will need to be reinforced as well as possible.

That is the basis of Defense-In-Depth (DID)–an approach to design, implementation, and operation 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. If all threats are handled at the level most appropriate, and DID is integrated in from the conceptual stage and not just added-on, then the effect is to aggregate the effect of defensive measures throughout the entire structure, benefitting from this blend of active and passive measures. These overlapping layers of protection should also integrate in the use of 'forcing factors'–a system element or process that requires the confrontation with the protection prior to the utilization of that element; this often requires the use of authentication, cryptography, judgment, etc. The DID approach can also be phased in, unlike 'rebuild' processes; as a new component is updated, it replaces older components (this obviously can take some time to replace worn-out or obsolete elements, but the advantage is that this is a process of continual improvement, as well as a componentized approach). While not perfect, it supplies a rigor of thought that provides an improvement over the prevailing approach, that of neglect of safety and security concerns, or coping with them as an afterthought. DID also requires a dedicated adherence to engineering rigor in all design: extensive testing, redundancy, graceful degradation with 'safe failure,' and essentially hardening of 'targets' in general. Notice that the collateral benefits are also considerable, leading to higher safety and improved quality.

The introduction of cryptography into the infrastructure is a politically sensitive point; the issue is whether access and utilization of strong, unescrowed ciphersystems in the infrastructure will not also lend security and protection to criminal elements, including OpFor. My belief is that the benefits outweigh the risk–OpFor already has access to strong, unescrowed cryptosystems from a variety of sources, while the infrastructure remains exposed to attacks. Certainly cryptography is not the answer to all IWAR threats–it doesn't protect the material infrastructure; it does, however, provide authentication and data security in the infostructure, which is of significant benefit.

There are also a few 'dangerous' trends (insofar as they create IWAR opportunity) in the infostructure worth mentioning, and which cryptography could have a strong role in risk management for. The concept of 'network' computer is entirely one of dependent machinery–a user would have no or minimal resources to fall back in the event of a network attack or failure. The increasing levels of homogeneity, particularly in hardware and operating systems, is distressing–heterogeneous information environments lend robustness (through protection against mass-scale uniform attacks), just as with genetic diversity in biological systems. Active/dynamic software, a logical extension of the object-oriented model, will soon make the prevalence of software anti-viral and security mechanisms worthless, as dynamic code and object-data execution make tracking of viral signatures nigh impossible. Ciphers

and data security could make homogeneous systems more robust (while still a bad trend), and cryptography will soon be an essential tool in combating viral and other penetration attacks (although for proper functionality, it will have to be placed directly on the motherboard, not in my opinion a bad thing).

TRUST

The issue of trust is going to be an increasingly complicated one, particularly as greater dependence upon the net as a component of the infosphere occurs. It is impossible for me quickly and easily to address this issue in a static medium, as concepts such as gradation of trust and the concept of reputation capital rely on very personal interpretations and reliance; it must suffice for me to say that as a global society, we have a lot to learn, and very little effort going into research, of one of the most important components of every social structure.

EDUCATION

Information and education regarding the IWAR threat should be widespread, as well as education regarding DID; the idea of 'security through obscurity' is self-defeating–if a system cannot survive open exposure and review, then the design is clearly wrong. Efforts to improve the community memory are crucial, since awareness of the threat is important to a DID strategy; this includes public education as well as professional, particularly in the intelligence, law enforcement, military, and civil communities.

SIMULATIONS

Part of the educational process should be the 'day in the life' exercise, as well as gaming and simulations of IWAR attacks. Gaming as a tool can affect individual and organizational decisions regarding planning, training, preparation, operations, and give critical insight into defending against IWAR.

Models and simulations, such as air flight simulators, can be reflexive simulations, oriented around providing experiential exposure to the participant. I personally prefer to focus on reflective simulation, oriented at cognition and contemplation regarding the subject matter. I have found that providing a continual experiential exposure at the reflective level translates into improved performance at the reflexive level.

Simulations and models can have serious flaws and drawbacks; there is a represented world (the real world) and a representing world (the world of the simulation), and design of the represented world and interaction within it is not trivial. Higher order representations tend to alter the relationships represented; models can leave things out that can't be represented, don't seem important, or for which no adequate constraint/limitation can be created. The representation is not the reality, which is why I don't believe that conclusions should be drawn from simulations, only lessons learned.

Done well, models and simulations provide `problem isomorphs' that capture the important and critical features; enhance the ability for understanding, judgment, and decision; and allow the participant to discover relevant regularities and structures. Simulations are a tool to aid in the management of complexity through enhanced group interaction, providing challenges, establishing goals and procedures, offering an opportunity for new interpretations, and the exploration of alternative courses of action.

Simulations also extend into testing, including the use of 'Red Teams' or 'Tiger Team' IWAR actions to gauge the success of defensive measures. This additionally expands the skills and knowledge of the offensive team; a good thing, as such tests and testing are only as good as the attacking team. Incidentally, this is one of the reasons why the knowledgebase in agencies of the U.S.'s defense establishment has been built by watching attacks on Defense computer systems–it not only 'tests' the

security of the systems and tracks the 'state of the art' in attacks, but trains the team working on IWAR attack/defense strategies and tactics.

SOCIAL ISSUES

OpFor happens for a reason–as I mentioned earlier, if you were to categorize personnel by political, profit, or pathological motive, then perhaps some of these can be alleviated. Not through the 'profile,' identification, and incarceration of potential IWAR OpFor practitioners, but through addressing some of the root causes. A general feeling of political disenfranchisement is certainly a contributing factor; the fact that crime pays, and pays well, reflects poorly on the state of social and economic development and opportunity; as for pathology, there have always been the mentally ill, but the dramatic increase in violence shows an underlying and disturbing social acceptance for the use of force or violence as a means to an end. All of these issues, and tough ones they are indeed, will need to be addressed before our societies and social contracts break down entirely.

OPERATIONAL ISSUES

As a set of societies at large, we need to understand that IWAR is not a problem created by governments, nor is it one that will be solvable by governments. The infra/infostructures and dependencies that are potential targets are civilian; there is very little indeed that is of 'government' origin, from paperclip to fighter jet. A free market emphasis on IWAR is crucial because that is from where the problem arises. This will translate into getting the free market involved, at least at the educational level to make them aware of the threat; defense-in-depth can't work without cooperation from those responsible for building and maintaining the infra/infostructure. Government efforts, particularly in the United States, are particularly inept–top-down, government oriented, totally misdirected, taking authority over an issue for which they can't possibly supply a solution.

What governments can do, after getting out of the way (for instance, on the cryptography issue), is to orient the law enforcement, intelligence community, and military in a way that will be helpful to a defense. The jurisdictional issues are the truly thorny ones–criminal violations or behavior should be dealt with by law enforcement; military issues or attacks should remain within the domain and control of the military (with some attention paid to the dependencies upon the civilian structure); intelligence should concentrate on the strategic and tactical efforts that undermine State strength and security, using workable tradecraft such as human intelligence, as IWAR doesn't show up on satellite photos or 'open source' collection efforts. One area which might best be managed at the governmental level, although that remains to be seen, is creation and operation of a specialized body for response to IWAR attacks (e.g., the counter-terror task force); if such a body could be 'above the disputes' that would arise in the professional community or private sector, then it might be useful. I personally cannot see any viability in governmental solutions to the IWAR issue; if, for example, the U.S. government had solutions or could have prevented the problem, then why didn't bodies like the National Security Agency (responsible, after all, for this sort of matter) do so? Either they have no more solutions than do we, or the 'classified' nature of such solutions precludes us from relying on their existence.

CONCLUSIONS

I set out in this paper to educate the reader, in some small way, as to the mindset of an IWAR OpFor professional; I have defined the conceptual basis of the strategy, explained some of the practical matters an OpFor faces in operation, discussed in a general way a variety of IWAR potential operations, given some 'food for thought' (I hope) with financial IWAR, and wrapped up with some concrete directions for application of a defense-in-depth approach to safety and protection from IWAR attack.

What I hope, more than anything else, is that the reader will be able to approach their own aspect of IWAR with a better understanding of how it all fits together, and even perhaps review history or operations to test their own mettle as well as the conceptual tools I hope to have provided you.

I have said before, and please let me reiterate it again: while IWAR is an old concept, the dependencies it strikes at are our own; if we refuse to address them, the consequences will be no one's fault but our own, but the effects will impact on everyone else related to us in the dependency network. Can we afford to let them down?

ABOUT THE AUTHOR

With 20 years experience defense, intelligence, information operations, corporate finance, and technology development, Mr. Wilson consults on matters of organizational safety and security, critical infrastructure protection, information security and assurance, intelligence, finance, and technology for multinationals and governments in Europe, Asia, North and South America, and the Middle East. As a pioneer and acknowledged leader in the fields of infrastructural defense, information operations, open-source and next-generation intelligence, Mr. Wilson is the winner of numerous awards, including the US National Defense University's Sun Tzu Award in 1997, and the G2I Intelligence Professional Award for both 1997 and 1998. In corporate finance, he structured multi-billion dollar merger and acquisition transactions for multinational clients. As a technology inventor, his inventions and development of various technologies include: computer security systems, anti-viral computer hardware, cryptographic methods, agent-based modeling, three-dimensional visualization and interfaces, and massively-parallel, massively-distributed processing systems. Mr. Wilson's educational background is in system theory, cybernetics, and general semantics, PERL (political science, economics, rhetoric, law), and physics. He can be contacted via email at info@metatempo.com.

