DECISION SUPPORT SYSTEMS, inc.

DSSI *METATEMPO: SURVIVING GLOBALIZATION*

IWAR THREAT MODEL

MICHAEL WILSON

DECISION SUPPORT SYSTEMS, INC.

INFO@METATEMPO.COM

HTTP://WWW.METATEMPO.COM

INTRODUCTION

Any discussion of the topic of infrastructural warfare, of which information warfare is a subclassification, must begin with an exploration of the threat. This is necessary for a multitude of purposes, among them an assessment of the validity of the threat, scope of the threat, probable activities of the operational force, and the necessities of a defense. At the time of the writing of this paper, the validity of the infrastructural and information warfare threat is being questioned in a variety of communities, including the military branches, intelligence community, law enforcement agencies, technical domains, media, and public. This spirited debate has dimensions worth noting:

- In the wake of the collapse of the Soviet Union, many who are skeptical of the threat believe that it is imaginary or manufactured to provide an on-going mission for the military, intelligence, and law enforcement personnel and budgets. This `creation' of a continuing threat is viewed as a mechanism for the justification of policies and programs that many had hoped would end in the dawning era of peace.
- The `cryptographic genie' has escaped from the bottle, and many members of the world political community, which the law enforcement and intelligence agencies must be viewed as part of, have been calling for on-going control of the technology of secrecy, privacy, and authentication. The rallying cry is "He who has nothing to fear/hide has no need of cryptography." Any number of public presentations have trotted out the Four Horsemen of the Internet Apocalypse–Terrorists, Drug Dealers, Pedophiles, Organized Crime. Multiple initiatives have been proposed and narrowly defeated that would limit access to enabling technology in cryptography, technology that would protect individuals and organizations from intrusion, espionage, theft, and other loss;
- Scare mongering, again on the part of political forces, has been used to progressively erode civil liberties with policies and procedures in the name of security, but which have no or minimal contributing factors to an actual defense. This further discredits anyone wishing to take a strong position acknowledging the threat, but against these sorts of measures;
- Top-down, blue-ribbon initiatives have been initiated that have as much hope of addressing the problem as legislating AIDS or drugs out of existence. As Churchill commented, don't mistake activity for action; political, law enforcement, or intelligence groups are damage control only. The problems of infrastructural and information warfare need to be fought where they originate–in the design, implementation, and operation of the key elements and structures targeted by attacks, commonly civilian in nature.

Considering all this, it is a daunting effort to provide a model of the threat. The protection against infrastructural and information warfare (referred from here on as I2WAR) is a defense-in-depth strategy–layered systems with integrated forcing factors, elements which require confrontation with security measures, to address each individual layer's weaknesses and maintain overall system integrity.

This sort of defense isn't built upon conceptions of a `single-threat' assessment, or even by being conservative when assessing the threat–it comes from viewing the opposition force as being almost mystically capable of delivering death and destruction. Defense-in-depth metaphors embedded throughout the political economy also address another key threat, the Lawrence Dilemma–T.E. Lawrence termed it as being able to protect any particular point against attack, but the inability of the adversary to protect every particular point.

Comprehensive threat models allow gaming against defense-in-depth designs, implementations, and operations to find and correct susceptibilities throughout the infrastructure, and encourage broad utilization of enabling technologies of defense such as strong cryptography; defense-in-depth gains strength from the aggregate of secure layers, making it easier to introduce the concept into the

marketplace and gain acceptance. Historically, this sort of approach to threat modeling and defense preparation has shown the greatest success–almost invariably the threat was something not imagined, but the variation and robustness of the defensive structures were better able to handle and eventually meet the threat which did occur. Underestimation and over-preparation are rarely either.

WAR AND INFRASTRUCTURE

Even a casual acquaintance with history will show that war and infrastructure have endured an interdependence across the centuries. Many of the ways that warfare is classified can be defined, in part or whole, by their effects on the infrastructure:

- Attrition warfare focuses on the collapse of the warmaking (force projection) infrastructure, with an eye on ruling the defenseless opponent. It may seem a primitive form of war, usually focused on the actual physical control of territory, and many historians point to World War I as the last great example; this, however, discounts the demand by the Allies for total surrender by the Germans and Japanese in World War II, and the subsequent occupation and political control (including limitations on force capabilities, removed in Germany for political purposes, still in force in Japan), as well as a number of more recent conflicts.
- Manoeuvre warfare seeks to control key points (usually viewed as the command and control structure), which it then uses as leverage to control the opponent on a greater scale.
- Guerrilla warfare emphasizes opportunistic attacks on military or political infrastructure; terrorist attacks emphasize opportunistic attacks on the civilian infrastructure; political warfare (polwar) seeks psychological impact on these infrastructures.

I2WAR is a synthesis of all of these forms of war, waged at a low intensity level. Society is supported by a vast network of interrelated and interdependent infrastructural elements, many of which are increasingly automated with technology partially or in total control, forming physical and `virtual' infrastructures. Just as there are two forms of infrastructure, the physical and the virtual, so have the attacks begun to focus on these varied areas of vulnerability–guerrilla and terrorist attacks on physical infrastructure, and what is termed `information warfare' (infowar) attacks on the virtual infrastructure. Attrition attacks correlate to the opposition forces' potential usage of weapons of mass destruction (WMD) or infowar denial of service (DOS) attacks; manoeuvre attacks are tactical operations launched against the physical or virtual infrastructures; guerrilla, terror, and polwar attacks are much the same, only now they utilize technology or target the virtual infrastructure.

It is, therefore, the model of an opposition force utilizing these strategies and tactics of I2WAR that is an essential tool to assess the threat and mount a defense-in-depth.

OPPOSITION FORCE (OPFOR) INTENT/MISSION ORDERS

What motivates the creation and operation of OpFor? Their agenda could be many things, but their purposes have commonalities:

- Damaging the basic trust of the citizens in the existing fabric of society; this may also include attempts to modify or replace the social system with new elements or in total (for example, communism, political Islam's sharia, Palestine, Ireland) but an OpFor may not be so ideologically advanced;
- Damaging the economy of scale in the social dependency infrastructure. All advanced societies have complex mechanisms that provide common support to significant portions

of the citizens (essential to the satisfaction of Maslow's Hierarchy–food, water, power, sewage, trade, etc.). Removal of this economy of scale, or dramatic impairment of its function, restricts the usage or benefit to the intended parties, and may trigger further collapse;

- Overburden and/or damage the law enforcement agencies and intelligence community elements responsible for protecting and maintaining the social fabric;
- Impair C4I (command, control, communications, computers, intelligence) with C4D (chaos, catastrophe, confusion, computers, deception–note that computers are a constant force multiplier in either domain).

These group motives and identities are composites and synergistic of the motives of the individual members, who may be motivated in even more varied ways, among them ideology, profit, revenge, seeking thrills and excitement, seeking recognition or power (potentially pathological), having `no alternative,' seeking group identity, or any number of unimagined reasons.

Categorization of OpFor is a dangerous thing to do; a primary problem is that poor assumptions would be made regarding the individual or group identity. A scale which may better portray an OpFor is phenomenological, particularly focusing on preference of attack profile–denial of service physical infrastructure attack, denial of service virtual infrastructure attack, psychological warfare attack, technologically augmented polwar–and the issue of scale–mass (large, coordinated, supported), strategic attacks; or leveraged (using time, intelligence-espionage, and intelligence-cognitive in small, uncoordinated, self financed), tactical attacks.

It is important to point out at this stage that there are two very different opinions regarding this issue of scale. One of the constraints on the model of the threat is that assumptions should be at their most generous, but which point on the compass is this? Much speculation on the I2WAR threat has included the concept of an information warfare `Pearl Harbor'–a singular sneak first attack that is brutally devastating. Is this in fact the maximum threat? The Pearl Harbor scenario seems very much to me an artifact of `old world' thinking, including the belief that the essential target of the attack and the sponsor of it would be governmental–some rogue State attempting to collapse the structure of Western power. Look at the actual Pearl Harbor attack–it was survivable, was costly in the short term but strategically a blessing (forcing a massive construction effort, as well as actually changing and improving the nature of the Allied naval force structure towards carriers), and aroused the national ire of the Americans (drawing them into the war, rather than knocking them out). Polar opposites of the Pearl Harbor attack scenario are on-going, low intensity, small, uncoordinated, tightly focused, self-financed and managed, guerrilla and terror operations aimed at a long-term attrition strategy (reminiscent of the Viet Nam strategy). Note that for the purposes of this paper, I choose this latter approach as the most threatening (evidence of the value of this approach will, I hope, be in the OpFor model I present).

OPFOR ORGANIZATION

Organizational configurations of OpFor groups are increasingly relying upon new metaphors made possible by current technology and derived from network theory; the old `cell' structure is replaced with star networks, or networks that look like fishnets. These organizational nets can be dynamically structured, have stable and mobile points, and may view all points as equal, with `command' being an agreeable arbiter or mechanism to gain perspective (a strategic viewpoint as opposed to tactical).

This form of organization is very much based upon functionality, and has `evolved' (in a `natural selection' sense) over time. Dynamic nets get `pulled' or distorted by the command node (grab a knot in a fishnet and support the net from it); this provides that command and control of the organization is dynamic, moving always to the micro-level and relying on the macro-level for perspective.

Management of the net becomes functionally based–essential domain knowledge is always resident, immediacy provides that command is always `forward,' and if there is coherent `baton passing' then heterarchies in tactical situations can act as dynamic `role based' temporary hierarchies. Given secure communications and information sharing through the heterarchy, the organization is a solid community memory, providing no weak central repository of authority, no Clausewitzian `centre.' In such OpFor groups every member of the group agrees on the definitions and intent/mission of the group unanimously (either by exclusion/removal of dissenting personnel, schism, or narrow definition of the group intent); in a heterarchy, authority is determined by knowledge or function, not position. Groups of this sort function well, as they are small, tightly directed, hard to detect, hard to stop, camouflage well, and the infosphere/information environment can accommodate any number `inside' the same physical and virtual territory.

ORGANIZATIONAL TOOLS

Certain tools need to be used according to a well-defined tradecraft to recruit for OpFor and communicate between member nodes. These tools can be accessed from any standard electronic account--anonymous remailer chains, newsgroups and search tools of such, world wide web pages and their associated search tools, ftp points, Internet Relay Chat and other chat mechanisms, multi-user domains, and mailing lists. In fact, operations can work entirely from electronic mail and Usenet news access, the simplest of mechanisms.

TOOL--CHAINED REMAILERS

Remailer nesting with cryptographic wrapping of messages is getting quite advanced, able to accommodate operational requirements with only a few additional operational requirements of tradecraft; in particular, the Mixmaster systems are very robust (see the URL http://www.obscura.com/~loki/ for Lance Cottrell's excellent work). The threat specification that went into design parameters is solid:

- All traffic in and out of all remailers is tracked (from, to, filesize, time in/out); - Traffic is backtrailed and forward traced to all known senders and receivers;
- An attacker has the same access to any arbitrary remailer as anyone else, and can attempt to flood any remailer with designed traffic, multisend captured traffic, or deny traffic (in part or whole);
- Some but not all remailers are compromised, and design specifications are known.
- The Mixmaster design addresses most of the issues of threats technically, and tradecraft negates the balance if OpFor tradecraft is adhered to as follows:
- Key sizes for public key messages (final `receiver' wrapper) is >= 1024 bits;
- Keys must be changed when a safe upper threshold of traffic using the key has passed; given recent disclosures regarding cryptanalytic attacks on public and private key systems, this threshold may be as low as 50 messages or 500K;
- At least six remailers are used in a chain to another e-mail account, at least three to Usenet news groups;
- Geographic dispersion should be selected so that one or two (in the middle of the chain) remailers are outside U.S. jurisdiction, preferably in more than one location;
- Latency and combined traffic levels are sufficient to provide decoy traffic, or decoy traffic must be generated by the remailer;

- Headers must be stripped, only the receiver knowing (or not, at option) whom the sender is pseudonymed as;
- Message IDs on messages with logging to prevent multisend attacks;
- Messages are split to uniform sizes to prevent filesize tracking.

OPFOR COMMUNICATION: NODES AND LINKS

A `paranoid' communication process between OpFor member nodes would be to only send through remailers for OpFor links, with the destination being a newsgroup used as a dead-drop. Messages could be obtained with no risk; traffic with a prearranged subject header would be encrypted with a group key, contain the message to the group or another embedded encrypted message to an individual node nym. This asymmetry of usage on the remailers would be picked up by a traffic analysis mapping across the remailers, which could be camouflaged by the adoption of a cover behavior (posting to certain newsgroups) or symmetric usage.

OpFor links could be established (recruiting) through the same forums with messages or offers intended to attract potential members. As such, operational rules of the group would again be along `paranoid' lines:

- Assumption that nodes in the net are compromised by LEA or IC;
- Nodes have entirely local management, control, information, planning, resources, capabilities, competencies;
- Net is to share knowledge, act as a `community memory,' not share operational plans or details. If the OpFor net is compromised by a penetrated OpFor node, what would the compromised OpFor node know? That the remailers are being used by an OpFor `group'; the private key for the OpFor group's public key messages; and the OpFor node's message traffic and stored data (assuming the private key is provided–and maybe not then, if a `flying dutchman' arrangement is made to keep incriminating files always on the move through the net). Penetration would provide no operational details, and no specifics on other OpFor nodes (unless they violated tradecraft), who can anyway drop from the net at any time tracelessly. Entrapment wouldn't be possible, as there would be, under tradecraft, no coordinated operations; turning the node or establishing a traitor node offers no benefit other than participation in the `community memory' of the OpFor group.

This system of organization provides OpFor a stable network of dynamic links between operational nodes, shelters the internals of the nodes (including substructures, potentially along other organizing principles, making this a sort of `intranet for terrorists'), yet acts to provide a sharing mechanism for knowledge. As new systems such as `electronic money' come into usage, the network also gains the ability to share finances and other resources between nodes. OpFor organization in this fashion provides the strongest position, greatest flexibility, and highest likelihood of avoiding detection, and should be considered as the probable structure forced by evolutionary pressures (natural selection–such structures provide the greatest probability of survival while maintaining operational capacity).

OPFOR RECRUITING

OpFor may or may not require a high degree of security and trust; either way, the cornerstone of OpFor relationships is the proper selection of personnel. Mechanisms to attract `like-minded'

individuals are the foundation of the Internet–newsgroups, mailing lists, web pages, forums for communication, virtual realities.

From this base a selection of potential members can be made using the intent and operational profile of the OpFor to set parameters of the recruit profile: skills, training, resources, access, character, etc.

Weeding this pool of potential members through a thorough background investigation is possible as never before for non- intelligence or law enforcement organizations willing to be operational for that purpose. Records such as phone, credit, banking, education, legal, travel, medical, and insurance are all obtainable; your average individual wags a very long electronic `tail' of documentation. Personality profiling can be augmented with additional data sources, such as video rentals, grocery purchases, or sniffing and tracking all of the subject's traffic.

The reversal of this process is also important–'legends,' or manufactured personal histories, can be created and seeded across the relevant databases. An OpFor can have access to any array of domain expertise, training, skills, monetary resources, access to desired information or locations, equipment; this fact destroys any elements of defense based upon restricted access to location, skills, information, equipment, etc.

OPFOR ARMAMENT

The destructive capacity of OpFor attacks using I2WAR strategies and tactics comes from more than armament or weaponry, but comes instead from the members of OpFor. It may seem odd to link people directly with weapons, but that begs the question, what is the purpose of a weapon? Weapons are about force, control, denial–some of the best work by implication, but real weapons aren't those you hold in your hands, but those you hold in your mind.

The best weapons, those that make men dangerous, are tools of thought–system analysis, operations research, game theory, cybernetics, general semantics, etc. Operationally speaking, knowledge and understanding of the opposition is the most important sort of information to possess (the Soviets even thought it a more important priority to control information regarding themselves over espionage against NATO targets). This comes from building cognitive models of the objectives, constraints, assumptions, dependencies, patterns, and complexities of your opponent. Game theory can be used to create and test scenarios, factoring in operational risks and consequences. Building and testing models is one of the primary functions of the technology embodied in the net; augmenting an operational organization, it acts as a powerful force multiplier.

Later in this paper I will expand on the utilization of cognitive intelligence as a direct factor of I2WAR; it should suffice to say that OpFor should be assumed to `outgun' their adversaries in the military, intelligence community, and law enforcement in this capacity. This is from the advantages OpFor may have naturally as individuals, their usage of technology for augmentation, the utilization of technology to create a `community memory,' as well as through their specialization.

OpFor ordnance may be along conventional lines or include weapons of mass destruction. Conventional weapons–whether explosives, missiles, mortars, firearms, etc.–are readily obtained by purchase or theft, can be manufactured, or made available in trade on the black market and through private arms networks. Unconventional weapons–nuclear, chemical, biological, informational–are not so easily obtainable, and require certain thresholds of skill and sophistication to acquire and use. There should, however, be no assumptions that such limitations or barriers will stop an OpFor from obtaining any military materiel they desire–recent years have shown that all conventional weaponry is available, nuclear materiel has `gone missing,' chemical weapons have seen use, technology and cultures

for biologicals have surfaced in the damnedest places, and informationals are beginning to surface in primitive denial-of-service attacks that prove the concept.

The will to use weapons of mass destruction is certainly present in OpFor; this issue has been questioned, particularly with the argument that it would be counterproductive, that OpFor wants mass terror, not mass deaths. Basing an assessment of OpFor will to deliver mass death based on the failure of delivery mechanisms is particularly odd, applying the logic of "that isn't a bug, it's a feature!" Mass death creates mass terror, but OpFor can use the results regardless of the final body count–weapons of mass destruction are a winning scenario, even when they fail. Acquisition and utilization of weapons of mass destruction pose an interesting problem to an OpFor–the more `physical' the brand of weapon, the easier it is for governments to control the elements needed to assemble one.

Nuclear materials and systems are regulated (or tracked as `dual use' technology), and chemical weapon pre-cursors (chemical building blocks) are tracked in quantity as well; both of these categories of weapon system are the common threat used to demonstrate the alienation of `rogue States' from the world community, but in reality, the control mechanisms on these weapons and related industrial base are considerable. Biologicals are less well tracked, and infectious diseases around the world can be acquired, quite easily and for a variety of seemingly `harmless' or even `beneficial' purposes by an OpFor; the physical requirements for work with biologicals are far less severe than for nuclear or chemical systems (although with far more complexities and complications), and well within the capabilities of a clandestine private lab. Informational weapons require only fairly inexpensive computer equipment, network access, and the domain expertise.

The `informational' value chain on the weapons–the knowledge and skill to build/use–is a parallel in complexity to the physical control requirements. Acquiring the know-how in any of the domains requires some advanced education–nuclear technology students are monitored and controlled to a degree, chemistry not nearly as much, biological knowledge is far easier to acquire (the instances of `physicians gone bad' are rare but notable, including Habash and Haddad), while the education regarding informational attacks isn't tracked at all. The level of sophistication required to mount attacks is at odds with the physical controls–atomic/nuclear principles are well defined and accessible, and even possession of nuclear material is a danger (scattered over a target, or introduced in some other primitive method); biological weapons require much more knowledge and skill on the part of an OpFor attempting their use; informationals, not taking into account `plug and play' attacks (construction kits, etc. which create basic attacks), require a considerable amount of specialized skill and knowledge to prepare and perpetrate.

Delivery mechanisms are similarly complex, with nuclear weapons having the most difficult of deliveries (missile, truck, assemble it on the spot), chemical being only slighly easier (aerosols, binary containers, etc.), biological (playing `hide the vector'), and informational being easiest (playing `hide the computer,' not very difficult at all). Damage (apart from threat value) from such weapons is congruent in complexity–nuclear/chemical are limited by their radius (and then weather), while biological weapons can have serious blowback effects, and informational weapons can either be targeted or have blowback if done poorly.

Given these elements of harsh reality, there are distinct limitations in OpFor potential usage of weapons of mass destruction–it would require a favorable combination of circumstance, resource, skill, knowledge, and delivery opportunity. OpFor usage of conventional weapons, with growing interest in informational attacks, begins to make sense–massive availability of conventional ordnance within the knowledge domain of OpFor personnel, evolving towards more sophisticated OpFor organizations still limited by physical access to advanced weapons materiel but who see informationals as an opportunity.

OPFOR INTELLIGENCE GATHERING AND ANALYSIS

OpFor–given expertise in using the Internet and other technological research tools, and operating in the same information environment available to most anyone willing to dedicate time, effort, and money to the problem–has considerable intelligence gathering and analysis capabilities. Using various tools to exploit this intelligence capability follows a fairly standard cycle.

INTELLIGENCE GATHERING

Tasking for OpFor gathering efforts begins with setting the objective; this requires an understanding of the target (and the footprints they leave), and the sort of intelligence desired: informational (political, industrial, economic, technical, personal) or behavioral (usually for the purposes of action forecasting, or to understand reactions and consequences to operations).

Enormous amounts of information are available to contribute to target profiles, a topic covered later in this paper. Methodology can utilize `passive measures,' activities that are normal transactions and require no special operations or privileged access to obtain. This sort of `net-based open source intelligence' (NOSI) comes from a wide array of sources:

- Active traffic and archived sources (these are highly opportunistic, and are largely traffic dependent);
- Database systems (Dialog, Lexis/Nexis, credit);
- Usenet news (and news search tools, by topic or author);
- World Wide Web (and web search tools);
- Mailing lists and other informal communication networks that are commonly archived;
- Media sources (news organizations, financial data, scheduling, etc.).

`Active measures,' those which require privileged access, or active queries which may betray the gathering process, are also part of the gathering methodology, but because of the risks they entail, may be less favored:

- Community memory, tapping into the knowledgebase available in the public virtual networks through active queries;
- Hacking/cracking, including the usage of session hijacking, IP spoofing, sniffing for traffic (intercepts), and traffic analysis;
- Human intelligence, whether witting, unwitting, or under coercion.

The gathering process can provide seemingly endless amounts of intelligence, with a number of recognized caveats–unknown provenance, `current reporting' emphasis (poor historical archiving and little qualitative data), accuracy (may not relate to ground truth), the fact that net-based data or models may not bear close correspondence to reality (for example, performance data), and that it cannot replace experience in a domain. Even with such constraints, later in this paper I will explain how it provides adequate data for OpFor purposes.

INTELLIGENCE ANALYSIS

The goals of analysis are to come to an understanding regarding the topic tasked in the process. This involves looking for patterns, relationships, interactions, dependencies, outcomes, consequences–not a task for the weak of heart or mind, as the true practitioner of intelligence analysis must avoid making assumptions or feeling he/she has the answers. Tasking on analysis for OpFor, beyond target research, revolves around forecasting–the possible/probable actions of targets as well as their perceived adversaries (military, intelligence agencies, law enforcement), and the consequences OpFor operations (for after-action management and propaganda purposes).

Forecasting is a mixed bag, for OpFor and Adversary alike–a belief in the predictive, probabilistic nature of the future is delusional, yet analysts persist because they're right often enough to keep them trying. The methodologies have improved over the years, evolving from single outcome forecasting (which requires considerable expertise and judgment, must relate to alternative predictions, but has the drawbacks of significant uncertainty, and the "you don't know what you don't know" problem), through Bayesian (iterative probabilistic) analysis (which takes into account previous judgments, but is as prone to error as single outcome methods, is too trend based and skewed by previous judgments, but is useful when judgment is solid, and there is no new information or new behaviors), to a more dynamic `continuum' methodology.

A continuum methodology, in practice among OpFor and conventional intelligence analysts alike, tracks actors/players using behavior mapping into a problem space (a position or options for a potential game turn) which relies on intelligence data–player preferences and goals, past behavior, stated policies, their perspective on the problem space, their cost-benefit ratios for various options, their capabilities and historical/probable resource dedication–for predictive purposes. The benefits of this methodology are that it is stimulus driven, allows multiple outcomes to be gamed, maps actors to positions, provides analysis by inference, takes in to account cooperative/contentive positioning of players, balances risks/opportunities for players and provides alternative options of potential action, and can vary factors (resources, game position, outcome priority) to experiment with a variety of scenarios.

OpFor has no significant handicaps in the domain of intelligence gathering and intelligence; the impact of this position can be seen where individuals with domain expertise and able to compare the fruits of large-scale espionage efforts and this sort of intelligence are increasingly favoring the latter. Additionally, as I will show later in the paper, this sort of intelligence for target research and behavior mapping is ideally suited to I2WAR, as opposed to traditional intelligence methodology and tasking.

OPFOR FUNDING

Conventional funding mechanisms (sponsors, donations, false fronts, etc.) notwithstanding, the wide variety of `net crimes' available for OpFor to engage in will likely provide any scale of funding necessary. There is no skill barrier to be overcome–much of the tradecraft and capabilities necessary to sustain OpFor lend themselves well to other ways of operating outside society and the law; it is no wonder that it is becoming increasingly difficult to draw clear distinctions between groups like OpFor, and those purely motivated by profit. Among the potential activities used to secure operating funds:

- `Computer crime' including break-ins, credit card fraud, cell phone cloning, phreaking (theft of service), and piracy can all be used to generate cash and provide capabilities to the organization;

- Blackmail takes on a new dimension through monitoring or sniffing an individual's message traffic and e-mail; monitoring of pipes to newsgroups or through anonymous remailers can provide leverage on individuals, forcing them to provide funds or information;
- Espionage can be directly engaged in, through break-ins, sniffers that monitor net traffic through the net, scanning e-mail, and other measures;
- Sabotage can destroy critical systems or data, or be used to cover for other operations; - Insider trading can be accomplished by monitoring financial activities of corporations or market makers and subsequent use of such information in trading (including use of knowledge of planned OpFor attacks, or selection of attacks with this intent);
- Money laundering becomes greatly enhanced by using modern technology, as does control of clandestine assets.

OpFor can rely on having access to any amount of capital they need, siphoned off from targets on a global basis; the strength of nations or transnational organizations make them particularly desirable targets, and can even combine the intent of the OpFor with funding operations. This lack of a functional restriction on OpFor potential funding impacts across its entire profile of capabilities, including the purchase of training/skills, equipment, information, influence, or anything else they may need or desire (and in fact this is an increasing factor in the attraction of such organizations to potential members).

I2WAR

Target profiles of I2WAR fall into four general categories:

- Denial of service physical infrastructure attacks, which can be viewed as low intensity conflicts, including guerrilla and terror actions;
- Denial of service virtual infrastructure attacks, what are being referred to as information warfare;
- Psychological warfare attacks, more subtle efforts that have their effect through perversion of the functionality of the decision-making process;
- Technologically augmented political warfare, which straddles the line of legitimate action in the political process.

Before discussing each variety of I2WAR, it would be fruitful to provide a process definition of what the infrastructure is. A singular definition is not possible–infrastructure varies from culture to culture, individual to individual, and moment to moment. What can be defined is the meta-process of defining the infrastructure for any particular instance of combinations, and how commonalities hint toward OpFor targets (and how, this process being used by OpFor, implies considerable intelligence^2 (espionage and cognitive senses) on the part of OpFor).

DEFINING THE INFRASTRUCTURE

Infrastructure is dynamic and varies widely across the individuals of a society. A working definition can be gained by the simple process of recording `a day in the life' of a significant subset of individuals--no need to be selective beyond a good, varied sample size, the process of set-building is self-correcting and self-identifying.

For a period in the subject's life, a record could be made of every service, object, mechanism, information, or process they take advantage of yet do not supply themselves. This record is a first-stage approximation of the dependencies the individual has on the infrastructural elements provided by the political economy. The elements on this first-stage list may be other individuals who are added to the process to contribute to the first-stage pool (probable additions would be skilled personnel such as physicians, attorneys, etc.); the process continues until all representative domains symbolized by an individual used in the pool have been added to the pool, or until certain practical limits have been reached. Thus the end result of the pool is a list of individuals and domains, and the material and informational dependencies they require to continue to function in their daily lives.

These dependencies are then the target of considerable research–ownership, functionality, work process, etc.–the very sorts of information most commonly available on the Internet and to passive measures of intelligence gathering. The goal of this stage is to develop the second-stage list of the functional dependencies of the prior stage; this is the second degree of separation from the population, and will contain organizations and mechanisms that the population at-large may not encounter.

This leads to the third degree of separation and subsequent research at this level, and so (the dataset tends to grow in links before it begins to shrink). Each stage in the process, the greater the degree of separation, provides a more detailed picture of the dependencies inside the infrastructure, particularly as commonality of dependency becomes more and more reinforced. What is eventually generated is a smaller and smaller list of common dependencies that are the critical points of a political economy–key points, choke points, bottlenecks. The process provides a mechanism to track backwards and forwards through the network built by degrees of separation, coupled with detailed intelligence data on specific nodes.

As a targeting tool for OpFor, it is unparalleled; to create an effect in a target (regional, domain based, demographically based, etc.), the dependency chain can be followed `upwards' (increasing the degrees of separation, but increasing the levels of commonality) until a weak spot is located–a critical dependency that the absence of would impair or halt the functioning of the target, yet which lacks protection from the specific capabilities of the OpFor. The targeting tree works in the other direction as well, where an identified potential target can be examined to see the impact on the subsequent elements (lower values in the degree of separation) of the political economy post-operation.

Scale is also variable, allowing targets to be selected on the basis of individual, organizational, corporate, or governmental profiling. Visualization for this method (which I refer to as the Nemesis Method and the data from it as Nemesis Webs) can be accomplished with a database linked into any one of the many World Wide Web browsers, or through a tool providing indented list processing (outlining) presentation.

The Nemesis Method and Nemesis Webs can illustrate weak points in political economies that are generally ignored–from just-in-time supply mechanisms that can be disrupted, key personnel in specific domains (such as intelligence agencies or law enforcement), or susceptible databases that modification or perversion have would have significant consequences. As such, let me discuss general areas of dependence, and how the four types of I2WAR would affect them.

DENIAL OF SERVICE ATTACKS ON THE PHYSICAL INFRASTRUCTURE--GUERRILLA WARFARE AND TERRORISM

Although the line between guerrilla warfare and terrorism has been blurred, they are still two distinct tactics of conflict.

Guerrilla warfare operations focus on military infrastructural elements, war material, money and finance, command-and-control elements, supply, and staging areas. Terrorism operations focus on recognition, coercion, intimidation, provocation, insurgency support, ambush, raids, assassination, bombings, kidnaping, riots, hijacking; these tend toward civilian targets, which is how they can be distinguished from guerrilla actions. Terror attacks have evolved. `First generation' terror efforts focused on an exhaustion strategy; targets were typically `no retreat' hostage situations, which eventually were successfully countermeasured with police methods and commando strikes. `Second generation' terror attacks aimed at recognition, a coercive propaganda; targets were and still are `no contact' profiles, with explosives being the weapon of choice, and countermeasures focus on the criminalization of the actors and actions, denying they have any valid political element. Historically successful mechanisms for ending guerrilla and terrorist actions have been through mitigation of the political circumstances that brought them about; this approach has in recent years been ignored, with the emphasis on non-negotiation with guerrillas and terrorists, and year after year the escalation continues.

As discussed in detail in this paper, the virtual infrastructure can be used by an OpFor to augment many of the elements necessary to guerrilla and terrorist organizations: organizational structures can abandon the obsolete cell structures, move to star or hub-and-star structures allowing direct control, only one level deep, yet with operational unit isolation if necessary for compartmentalization; cut-outs, drops, and forwards with chained remailers; communications gain security and authentication with the use of available cryptosystems; recruiting becomes voluntarist, and allows deep background investigations and legends/covers to be created; training can be managed with multimedia tools and virtual reality simulations for operational walkthroughs; funding can come from the net, or be laundered using it; the net can become the weapon with infowar attacks; conventional targeting is aided with target profiling and research; propaganda and spin control can be managed through the net to prevent media control by intelligence community and law enforcement sources.

Physical infrastructure denial of service targets are probable along the following lines:

Communications/Media

Based on how you view I2WAR, communication channels are either the primary target of a large scale attack, or unlikely to become a target. Advocates of the position favoring massive attacks (the `Pearl Harbor' scenario) have a point–the direct and collateral damage that would be caused by a communications outage would be significant, but the situation would likely be corrected inside of a span of hours or a few days. The communication system was built to be robust, on both a physical and virtual level; any actions requiring the `cover' provided by a communications blackout would need to be operating on a fast OODA cycle and have considerable impact.

The contrary viewpoint is that attacks on communications systems (if not narrowly targeted, such as specific switching points or towers) and the media are counterproductive–the systems are necessary for smooth functioning of OpFor organization, and communication of the messages and actions of OpFor operations. Media outlets are an OpFor force multiplier when used correctly and to OpFor advantage, and the media provide their own sizzle. OpFor understanding of the media process/techniques (media `hot' and `cold') and media markets is probably quite sophisticated.

For example, operations may be deliberately launched in geographic locations `in the middle of nowhere' because there is no media middle-of-nowhere thanks to modern communication technology, yet middle-of-nowhere locations will have little to no other competing news events. The scenarios regarding this element alone are the most significant schisms in the discussion of I2WAR strategy and tactics.

Power Infrastructure

Generating plants and delivery systems for the power grid are not exceedingly robust, and trigger their own scale-back or shut-down once outside of stringent tolerances. Denial of service attacks are indirect, with their real impact being the collateral outages of services, but have the virtue of being simple to effect.

Water

Given the scares of drugs in the water supply in the 60s and 70s, processing plants are relatively secure; yet nature has found the weakness with extremely resistant microbial organisms which are not difficult to obtain/culture, and once introduced into the system, have considerable direct and collateral effect. Massive culturation and introduction of microbials requires limited skills, equipment, and capital investment, leaving this infrastructural element as a potential target for a WMD strategy.

Fuel

Numerous, reasonably accessible targets are available–tankers, pipelines, storage, gas stations, propane storage, tanker trucks, etc. Not difficult to ignite, such sources provide considerable fire and explosive hazard; planned effort to attack numerous sites could have frightening effect.

Banks

An essential part of the currency cycle, banks are harder targets from security and surveillance standpoints. Subtle attacks of information warfare or through propaganda (bank runs) may be more likely, but creative actions may also be possible (for example, a `malfunctioning' automated teller `giving away' money would attract quite a crowd, which is then susceptible to violence from an explosive device or weapons of mass destruction).

Markets/Exchanges

These are potentially more susceptible to infowar attacks, but are among the hardest targets from any denial of service perspective. Historical evidence suggests that operations employing considerable force or weapons of mass destruction may actually have potential for success.

Air Travel

Circumvention of air/airport security continues on a regular basis; only the non-functioning airport can be considered secure. X-ray/metal detectors rely on personnel, and can be fooled by devices with little or no metal; bomb detection devices look for chemical trails which only changes the selection of the weapon, from nitrogen-based explosives to chemical or biological weapons for instance; cargo containers to withstand explosions can be negated by binary packages, combining thermite to burn through the container with a device to explode after a delay. Security procedures securing airports have little effect; too much traffic, ease of obtaining false ID, etc. make airport security procedures an exercise in wishful thinking.

Rail

Highly attractive targets, rail travel is poorly controlled, easily accessible across the railsystem, and regularly carries harmful or dangerous substances in, through, or near populated areas.

Ground/Public Transportation

Free access with minimal effective control makes the delivery of car and trucks bombs relatively simple; tunnels and bridges are particularly vulnerable. Bussing and commuter rail/subways are similar targets for explosive devices or weapons of mass destruction.

Schools/Religious Institutions/Administrative Facilities

Ease of public access and the trust of those using the facilities makes them targets for disguised bombs, booby traps, and weapons of mass destruction–toys or lunch pails with explosives on a playground, or an attack on a regularly scheduled religious service, etc.

Emergency Management Systems (Police, Fire, Ambulance)

These groups are particularly susceptible to attack, and provide high-profile media coverage; anti-personnel booby-traps or firestorm mechanisms could overwhelm EMS personnel, and provide reluctance of other EMS personnel for continuing their operations. Ecological warfare (for instance, a plane dropping chemical-timed thermite pencils while flying over a region, or targeting refineries and chemical plants) is also possible.

Business (Food, Medical, Misc.)

The public dependence on such providers makes the impact of product tampering, explosive devices, or weapons of mass destruction particularly leveraged. Shopping malls have near perfect target profiles for weapons of mass destruction or explosive packages.

Public Events

Concerts, conventions, sporting events, etc. are venues with existing media coverage, large crowds, and easy access for explosive devices, weapons of mass destruction, or other attacks.

Government

Little benefit is to be gained by targeting political figures or organizations–the myths and romanticism surrounding the political domain make martyrs out of any attack. OpFor nodes wishing to have real effects on society or organizations need to recognize that political figures have very little `value add' to society, and are best left in place to add to the confusion. Law enforcement agency and the intelligence community personnel are open to serious and subtle attacks, ranging from identity hacking (use or damage to personal data) to using such data to select and target true `value added' personnel for elimination.

DENIAL OF SERVICE ATTACKS ON THE VIRTUAL INFRASTRUCTURE--INFORMATION WARFARE

Many of the same elements of the physical infrastructure are also maintained by systems connected up in a virtual infrastructure, and attacks on this aspect are referred to as information warfare (infowar). Potentially effected infrastructural elements include: telephone communication networks and collaterally reliant systems, such as emergency services; power grid, water, and sanitation management; financial networks, including automated tellers (ATMs), credit cards, debt and equity markets; technology related or dependent industries, from hospitals to airlines; media organizations; transportation network coordination; government agencies, from social security to the intelligence and law enforcement bodies. Any of these systems could be targeted by an OpFor infowar attack.

Why is infowar possible? While the real world has numerous inherent constraints and limitations, the digital world is infinitely malleable–the burden is on the user/observer. The organizations that have become dependent on the technology of the net have placed their trust in their systems, even though they are insecure and not always reliable, because they have had no choice. Automation has become the only way for such organizations to expand their functions and capabilities (from international switching of phone calls to clearing a credit card from half-way around the globe). But what technology gives, it can also take away.

Information warfare will likely play a part in some future military conflict along conventional lines; the point of the attack will be denial of service of some elements in the military C4I chain (command, control, communications, computers, intelligence). Given U.S. reliance on C4I as a direct force multiplier, it stands as being one of the most probable first targets. Such attacks will take technical sophistication as well as access to knowledge (and possible physical access) of C4I systems, not something casually gained. Massive infowar attacks such as the postulated infowar `Pearl Harbor' would, almost of necessity, be linked to some sort of high-intensity military conflict–no other rationale for them makes sense.

Infowar is still properly viewed as an element in low intensity conflict, independent of conventional military operations because of the advantages infowar attacks provide: they are highly leveraged, have a low cost of entry, don't require being in any particular location, are both strategically and tactically useful, have an extremely high tempo, make up for a lack of numbers or resources by substituting time and inventiveness, are hard to monitor capabilities or detect attack, provide both moral and material surprise, can be synchronized or simultaneous anywhere in the global virtual infrastructure, and have an extremely high value in damaging the morale of the opponent.

There are, however, interesting comparisons and parallels between the factors of conventional warfare and infowar: they both strike at the dependency infrastructure and value chain, although at different levels; ground/terrain concerns become issues of the infosphere, infostructure, connectivity, and non-local capability of attack; tempo gains directly and in simultaneity; leverage comes from targeting and the ability to `pre-load' the attack; mass equates to processing power, time, and connectivity; readiness is preparation and planning, and adds preprogramming; security as always is security, timing, penetration, and cryptography. I believe it is these interpretations of infowar capabilities that contribute to the continuing viewpoint of military infowar attacks, including the `Pearl Harbor' scenario.

Whether high or low intensity, infowar attacks use the virtual infrastructure directly as the weapon or target, and this is unlikely not to be exploited by OpFor.

PSYCHOLOGICAL WARFARE ATTACKS

More subtle forms of infowar target the data and information used in the decision making processes necessary in the political economy. Intended either for direct effect, or to undermine the psychological reliance and trust on the databases of the political economy, psychological warfare attacks have every bit of the power as denial of service attacks. Data provided to a professional in the course of their work has some very odd trust values–such data has `reputation capita'` as if it could be relied upon almost without question (even though errors are common).

Access to data in domains such as medicine, legal, law enforcement, or financial (to name a few) sectors are readily susceptible to perversion in dangerous or catastrophic ways. Changing a medical history or medical lab data could be life threatening; alteration of case law in legal databases could have significant civil rights impact; alteration of a police file could clear a dangerous felon or turn an honest citizen into a wanted cop-killer; financial data alteration could wreck an individual's credit rating,

improve a corporate rating to obtain a loan the company plans on defaulting on, cause a `run' on a financial institution, etc. No mechanisms are in place in databases to provide for accountability or authentication of the data they provide. A strong solution, the introduction and utilization of strong cryptography, is long overdue; this issue, in fact, is one of many reasons why strong cryptography should be available in the marketplace.

Government resistance to strong cryptosystems, through legislation restricting such things as key-length or proposing key escrow, imposes a seriously flawed trust system. Even the very idea of key escrow is contradictory: it requires a weakened cipher, a weakness by creating a targetable key repository, leaves open the issues of trusted access to the escrowed keys, and totally undermines reliance in an open political economy in the trustworthiness of authentication and cryptographic signatures. Strong cryptosystems as background enabling technology would act to prevent virtual infrastructure denial of service attacks, stop the spread of computer viruses and worms, limit industrial espionage by improving secrecy, provide a backbone structure to secure private data in databases (requiring keyed permission for approved access), and provide authentication and accountability inside of databases to limit the effects of psychological warfare attacks.

OpFor has a growing target space for attacks as more and more databases are utilized regularly to make decisions in the political economy; in this case, they have the tacit cooperation of the political forces arrayed in favor of weak or escrowed cryptosystems.

TECHNOLOGY AUGMENTED POLITICAL WARFARE

Political warfare straddles the edge of being part of the `legitimate' political process; it still merits consideration, however, as certain elements of polwar have been altered of improved radically by the introduction of technological augmentation. OpFor may or may not choose to utilize tools bordering on the legitimate, but the possibility cannot be discounted.

AGITATION, SUBVERSION, AND RIOTING

Revolutionary movements need to build the support base of disaffected societal elements; it is this core that establishes political momentum to a `movement' and acts as an example for potential new members and the society at large. Mechanisms such as the Internet provide an ideal tool for management of this base: members can be educated through the medium of the net; they establish alternative structures for civil, police, and military matters; and they can organize events and initiate `flash crowds' (spontaneous actions) designed to disrupt the existing social system and attract recruits to the movement.

Sophisticated targeting and profiling of the support base can supply leverage along Pareto simplification–effect the twenty percent of the social structure that creates eighty percent of the social support and stability.

PROPAGANDA, PSYOPS, DISINFORMATION

Propaganda and psyops efforts have a ready tool in technology. The digital nature of modern media makes many psyops efforts easier, and introduces a few new tricks. `Mobile truth,' or the reinterpretation of events (revisionist history), is a common feature on the Internet, which is increasingly becoming an entry point into the more conventional media and a key component in the `information environment' of a growing segment of the population.

Psyops in support of OpFor operations, including spin control, after action reports, or informative accounts when the media is (perceived to be) controlled by intelligence and law enforcement, are increasingly occurring using modern technology. The digital nature of media–text, photographs, video, audio–has undermined the ability to establish the reality of what they represent as observational proxies (creation of false digital evidence has recently been referred to by the U.S. military as the `fictive environment'). OpFor is unlikely to not take advantage of the propaganda and psyops opportunities made possible by technology.

PHILOSOPHICAL INTERLUDE--WHY IS I2WAR POSSIBLE?

The potential of I2WAR was made inevitable by the way in which advanced societies evolved mechanisms to cope with complexity and their own continual advancement. As systems were developed, decisions were made in favor of speed, convenience, and ease of use, rarely for overlapping layers of security measures for a defense-in-depth. Even now, physical attacks in the real world–at choke points, bottlenecks, key points–are easier for many to `get their mind around' and understand their impact; denial of service and perversion attacks may not be so easy, and merit further explanation.

Denial of service and perversion attacks, those which seek to impair or incapacitate by removal or alteration (even if only temporarily) of some critical component of the infrastructure, are actually attacks on the control and decision processes, removing the benefits of automation and economy of scale from the loop. Understanding requires a little knowledge of computers and cybernetics.

Computers, at a very basic level, are calculators. The most basic of computers, a Turing Machine, functions along a linear mathematical process performing programmed functions. Modern computing has its roots in the Manhattan Project, where teams of humans then eventually machines were essential to calculating specifications for the atomic bomb. The next generation of computers added a dimension (in conceptual modeling of a data space) to turn computers into virtual pieces of paper–more dynamic and with more functionality, great for things like word processing and spreadsheets. Computers still have the same purpose–they are tools to model reality, and the better the model, the more they can help us work on real world problems.

Since many of the metaphors for thinking and communicating about reality are planar, the move to planar models in computers was natural. Why stop there, however? Computers can handle many more dimensions, so tools like multimedia or virtual reality are worthwhile–three dimensional representations that are dynamic in time. The closer the internal representation in the computer can model external reality, the more useful the tool.

A principle of cybernetics is that any control mechanism, whether a simple thermostat or something complex for a nuclear power plant, have a model of the system being controlled as a component of the `governor.' Simple vector computers can monitor, model, and control many varieties of processes, allowing what is termed automation. As computers and models become more complex, adding dimensions and the ability to be dynamic, we have begun to use models in more interesting ways; they can now be used to generate options or recommendations, either for human or automated judgment. Pressures of managing complexity under the immediacy requirements of `real time' have fueled demands for increased automation, increasingly putting human judgment secondary or out of the loop completely, trusting in the computer and model to function as the best manager/governor in real time.

And therein lies the problem–attacks on automation can force the failure of the process; an economy of scale in management through automation lost leaves the burden of management entirely upon the unaugmented human element, who are hard pressed or unable to manage the scale, speed, complexity, etc. This is the essence of denial of service attacks on virtual infrastructure elements.

Perversion attacks are far more insidious–by altering or damaging the model in an undetected fashion, the decisions based on the model will fall out of step with reality. Small or aggregate changes can cause disastrous errors of judgment, the selection of options or recommendations that are at odds with `ground truth.' Arbitrage, or taking advantage of this model-to-reality difference, can be a calculated element of an adversary's deception operations. Computers and models can be powerful tools–and can also be turned into powerful weapons to incapacitate the user if they are taken away or used to lead them to disaster.

CONCLUSIONS

An assessment of whether the I2WAR threat model is accurate and/or useful is the responsibility of the reader; as the author, let me summarize the argument:

Validity of Threat

Nothing discussed regarding OpFor in this paper is not currently possible or actual; there are no barriers or constraints in the establishment or operation of OpFor exactly as outlined. I did not exaggerate the case for potential capabilities of the OpFor, finding that the optimal case for OpFor also happened to be strikingly similar to the `mystically' capable organization. The intent of OpFor is an abstraction of any number of operating philosophies of radical groups; the organizational structure and methodologies are in fact being utilized; the practices of attracting and clearing recruits are no more unbelievable than the fact that many intelligence and law enforcement agencies practice the same, perhaps with less thoroughness; the armament for OpFor makes them as dangerous as anyone can be, if they merely use their mind as a weapon; the intelligence gathering and analysis capabilities are well suited to the uses OpFor will put them, and in fact are probably more useful than that of their law enforcement or intelligence adversaries; OpFor funding assumes nothing more than that a willingness to break the law can be quite lucrative.

OpFor can be real; disbelief only makes more potent the surprise of their actions.

Scope/Activities

The exercise of mapping the infrastructure is a worthwhile one to engage in, for both sides of the struggle. Attack profiles–denial of service attacks on either the physical or virtual infrastructure, psychological warfare attacks, and technologically augmented polwar–are rich and varied, and show the depth of the susceptibility to an OpFor.

Defense Against I2WAR

The elements of a defense against I2WAR begin to become recognizable in light of the threat model, demonstrating that a well discussed problem contains the seeds of the answer; some of the most important, in my opinion, are:

- Map the infrastructure, calculate the dependencies; I provide an introduction to the methodology I use (the Nemesis Method of mapping Nemesis Webs), and I urge the reader to map their own, following the exercise through to see where it leads. They may be surprised;
- Address the intent issue of an OpFor; the numbers of disaffected, disenfranchised, and disgruntled are increasing everywhere; governments and social structures no longer seem to be in the hands of the people (or never were), and the Rights of Man are rapidly becoming privileges granted by the State. This trend either has to be reversed voluntarily, or will lead to its logical conclusion;

- Launch an effort to establish a defense-in-depth with graceful degradation; introduce forcing factors, security, and authentication into the design, implementation, and operation of the elements of the infrastructure. This isn't a top-down government-driven approach, but intended to address the threat at the point from which it originates, in the free market;
- Security through obscurity doesn't work; the public at large, and those responsible for the infrastructure in particular, need to be educated regarding the threat and how they can contribute to a solution at their level. It might not seem like much, but such effort adds up;
- Make strong cryptosystems available and easy to use; the concepts of privacy, security, and authentication are critical to a defense against I2WAR threats, not to mention a host of other issues (industrial espionage, crime, etc.). Banning strong cryptographic technology doesn't deny it to OpFor, but does limit the use of such systems for defensive strategies. If governments won't help, then they should at least get out of the way;
- Leave the law enforcement agencies and intelligence community tasked as they are; many of the elements of the I2WAR threat are already within their scope, including the variety of criminal actions involved in preparing for or carrying out operations. The bodies should concern themselves with the subversion that leads to destruction, not insinuate themselves into situations where there are no victims.

Final Word

I believe I have satisfied the requirements of building an accurate, robust model; I assert that I make the case for the validity of the threat, the probable scope and activities of the OpFor, and how defensive tactics begin to become apparent. I expect this model and particularly my recommendations for a defensive strategy to be controversial and come under attack; anything less would prove to me that I hadn't gone far enough. If you disagree, and decide not to prepare to meet the threat; I wish you luck. If you agree, in whole or part, then the time to do something is now; every day that passes is another day of exposure, another day that goes by when elements of the infrastructure could be improved or replaced with secure, trustable systems. Don't just stand there, do something.

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.

NOTE: This is a re-release of this paper which was published in 1996 by 7Pillars Partners. Permission was granted by 7Pillars Partners for this re-release. 7Pillars and Michael Wilson retain all copyright and intellectual property related to this paper.

