DECISION SUPPORT SYSTEMS, inc.

DSSI *METATEMPO: SURVIVING GLOBALIZATION*

CONSIDERING THE NET AS AN INTELLIGENCE TOOL

OPEN-SOURCE INTELLIGENCE

MICHAEL WILSON

DECISION SUPPORT SYSTEMS, INC.

INFO@METATEMPO.COM

HTTP://WWW.METATEMPO.COM

"...it being my intention to write a thing which shall be useful to him who apprehends it, it appears to me more appropriate to follow up the real truth of a matter than the imagination of it; for many have pictured republics and principalities which in fact have never been known or seen, because how one lives is so far distant from how one ought to live, that he who neglects what is done for what ought to be done, sooner effects his ruin than his preservation; for a man who wishes to act entirely up to his professions of virtue soon meets with what destroys him among so much that is evil. Hence it is necessary for a prince wishing to hold his own to know how to do wrong, and to make use of it or not according to necessity."

–Machiavelli, The Prince

INTRODUCTION

While the net is still in its infancy, already the potential for its use as an intelligence tool is becoming widely recognized. It is worthwhile to explore the actual scope of exactly how useful and in what areas the net will apply in. A good place to begin such a discussion is with some definitions of terms; all things being equal, I will start the defining process with the terms in the title of this document. [Please note that this document is a 'consideration' of the potential and capabilities offered; as such, it paints a broad stroke and sacrifices detail. A roadmap for the serious practitioner is presented, and should suffice to advance his or her own thinking on the matter.].

THE NET

Of all terms to be used in this document and the media in general, the most broadly defined is the 'net,' 'cyberspace,' or whatever the term-of-the-week is. For the purpose of this document, the 'net' is the virtual communication structure made possible by a very simple but fundamental conceptdata is data. Once something is reduced to digital format, it doesn't matter what it 'is'--text, graphics, photos, audio, video, all flatten into Turing-level bitstreams that the observer needs to properly interpret (referred to as 'reader makes right'). This concept is the force merging the old phone companies with cable companies, with content companies, with cellular phone companies, with Internet companies, and so on. What becomes important are the features of the connection between communicating parties–throughput, bandwidth, interactivity. "How fast are you? How dense?" So we see that the net has many featurestelephones, public and private, short- and long-lines, cellular; telephone related tools, such as pagers, facsimile machines, voicemail; interaction metaphors that exist in the network, such as electronic mail, bulletin boards, mailing lists, newsgroups, chat mechanisms (IRC, chat 'rooms'), multi-user

environments (MUDs, MUCKs, MUSHs, MOOs), gopher, the world wide web, archives and search tools; virtual communities and voluntary associations, such as cypherpunks; network tools, such as remailers, public-key cryptosystems, security packages, authentication mechanisms, reputation markets; and a variety of community input/output tools, such as scanners, printers, wire/information services. The net isn't just about communication pathways, but also about computing resources. 'Data is data' isn't enough; you quickly find out that everything is local--raw computing power and data storage are going to be available, any user in the net can have access to as much of either as they wish. Communicating parties can be anywhere. The channel has grown up to be diverse, complex, and robust; content is anything that a representation of can be generated in digital format. As a result, the enabling tool--the computer--is becoming more than a modeling system for old 'paper' applications (two-dimensional constructs such as spreadsheets and word processors), and transforming into an integrated piece of the dynamic, multi-dimensional representations. It is Project Augment writ large. This is the net--a fluid domain of ever-shifting patterns of links and nodes, parties exchanging bits of this and that, things that may represent the real world, or have no worldly connection whatsoever.

INTELLIGENCE & TOOLS

Two senses of the term intelligence will be used in this document. Intelligence can be the discovered/acquired variety, such as espionage, and I will also link the domain of operations, even though this addition is a common misconception. There is also cognitive intelligence, which allows us new ways to think about things; to limit the discussion, I will only use this interpretation in conjunction with the first sense of the term.

In the combined kingdom of the intelligences, information is what it is all about. Accurate information effects risk, allowing it to be predicted and prepared for. Information creates and then degrades models, for nothing stands still. Information mechanisms create new abilities for deception through the creation and manipulation of 'truths.' Jointly, all of these create opportunities for arbitrage, playing the appearance of reality off against what actually is real.

Tools are systems, processes, or mechanisms that allow, support, enhance, or amplify an ability. As such, tools can be hard (wedge, lever, screw), soft (computer applications, the communication network), or wet (cognitive concepts and abstractions); increasingly, human tools are rooted in all three domains.

AN OBSERVATION

Keep in mind while considering the net as an intelligence tool that the main beneficiary and main target for some time to come will be the United States of America. The reasons for this are an interesting twist on an old metaphor. One of the primary justifications for governments is that they act as a redistribution mechanism for the wealth of the governed; depending on the form of government, much of the spending is oriented in varying proportions at 'guns' (defense spending) or 'butter' (social programs). As economics has become a more obvious factor in international power and prestige, investments have been made in 'cows,' or mechanisms that kick off cash to be spent on guns or butter. The inefficiencies of government planning and spending aside, the Law of Unintended Consequence paid off for the U.S. investment in the net; by accident, this cow is paying off in both butter and guns (as a force multiplier, e.g. the Gulf War/Desert Storm). But guns and any technology in general are tools, and tools are value neutral--their use defines their 'moral' value.

ESPIONAGE

Espionage is the process of gathering or receiving data by clandestine means. By definition, espionage is illegal; it is a process of breaking laws to gain intelligence data. What sort of intelligence data is this? Strategic? Tactical? Economic? Political? Social? Technological? To be flippant, 'Yes.' All of this sort of data can be illegally gained from the net, and increasingly so. Espionage targets are commonly communication paths–it is hard to pull this kind of information out of peoples' heads, so you have to wait until it is being communicated, and the net is rapidly becoming a primary form of communication.

Superficially, human intelligence (HUMINT) looks like espionage, but by definition, HUMINT requires a certain level of cooperation to gain much of anything useful. No, communications systems are either the enabling tool for humans, or the mechanism of their spectacular indiscretion. Signal intelligence (SIGINT) has, therefore, become the primary focus of espionage work in modern times; attacks on communications systems were always a Soviet priority, and the U.S. designated considerable resources as well, particularly in the vehicle of the National Security Agency (NSA).

IS OPEN SOURCE INTELLIGENCE (OSI) ESPIONAGE?

The Central Intelligence Agency (CIA) Scientific & Technical Analysis group recognizes many mechanisms for gathering intelligence: photo intelligence, signal/communications intelligence, technical intelligence, foreign literature, proof-of-concepts demonstrated by U.S. work, and the fundamentals of reality that apply for us all (physical laws, mathematical properties). HUMINT plays against these many mechanisms in a continual tug-of-war for those evaluating and analyzing intelligence datacontext vs. objectivity, quality vs. quantity, speed vs. accuracy, security of the source vs. use of the data, intent vs. realized actions. Because of the burden associated with such evaluations, considerable effort is put into gathering from open sources, those for which no illegal action is necessary to derive data from. Historically, diplomatic services have concentrated on gathering this variety of data, and with good results; clandestine services have regularly augmented their regular espionage activities with OSI data, or in certain instances, relied upon it completely. Reasons for this vary, but trends point to the intelligence product customer's desire for current reporting. Espionage is a low volume, but more long-range 'intent' driven intelligence; the political consumers of intelligence data "don't have the time" for the development of clandestine intelligence sources.

Much of what is readily available on the net is 'current reporting' sorts of data–perishable, high volume information about what is going on right now. If viewed as a linear spectrum, on one side is HUMINT, the most valuable data when accurate, because it can tell you why rather than just what, with long term implications. Down the spectrum, you hit SIGINT; being a 'fly on the wall' party in a trusted exchange of communication can yield valuable data, but you have no control over topics or flow, it is purely a target of opportunity. Eventually, at the other end of the spectrum, you hit OSI–historically shown as useful, but totally beyond your control. Don't mistake the part for the whole; OSI is not espionage, and only a part of real intelligence. When you start combining the net with the concept of OSI, it begins to look very attractive, seductively so. Plenty of current reporting, good data, and dirt cheap; it is like being on the receiving end of a fire hose, so much data is pouring through the net.

OSI on the net has a number of flaws, however:

- What is the provenance of the information? What do you really know about the source?
- The noise vs. signal ratio on the net makes the analysis job a unique task, and almost requires that OSI be viewed only as supplemental to HUMINT and espionage sourcing;

- There is no 'pure' data; everything is either perverted, skewed, cooked, filtered, or outright manufactured;

- You get what you pay for; given that you're sitting on the receiving end of a fire hose, what is the benefit to the source in releasing the data? Playing the game of 'who benefits' is necessary to assess OSI;

- Given the information overload difficulty (ever try drinking from a fire hose?), filtering is essential on the analysis end, including automated pre-filtering, but there is the unlikelihood of any serious operator following tradecraft using keywords in the clear;

- How do you summarize the output of a fire hose? Given the level of dynamic data, you can't keep pace with an iterative review of continual reassessment;

- Large bodies of real-time current reporting are useful, but have real drawbacks; decisions tend to get made prematurely, and based on data with all of the aforementioned drawbacks. Net-based OSI (NOSI–pardon the author's weakness for horribly appropriate puns) does serve a useful function of augmenting research, but should not be relied on as a single source, or be used to substitute for real espionage or operational capacity. NOSI can however be useful in providing different viewpoints and to contemplate and prepare for widely varied scenarios.

A BRIEF INTERLUDE

I would like to briefly point out the egregious, delinquent behavior on the part of the intelligence community and law enforcement agencies. The debate over strong cryptography has been, at the time of this writing, waging for many years. The governments of the world would seem to want to outlaw strong cryptography, or make weak, key-escrowed cryptosystems the de facto standard. They point out many reasons for this, including the potential use of strong cryptosystems by drug dealers, terrorists, child pornographers, and criminals of any ilk. These same people are also the ones who point out that industrial espionage is occurring at an alarming rate, and guesstimate losses over $100 billion (U.S.). For some odd reason, they don't see the connection. Free availability of strong cryptography that is easy to use would go a long way toward protecting everyone's secrets--governments, corporations, individuals. The criminals will have it too, just the way they have computers, and pay phones, and automobiles, and a number of other potentially deadly tools. One of the strengths and inherent dangers of freedom is that the citizens have the opportunities to be responsible for and to themselves, without Big Brother or Big Daddy 'protecting' them from themselves. The issue for governments isn't about their citizens' freedom--the real issue is that they have spent considerable time, money, and efforts to develop SIGINT intercept tools. The longer they resist strong cryptosystems, the longer all those old tools still work. Once strong cryptosystems come into regular use, all those high-tech espionage tools go the way of the dinosaur.

PROCESSING

Distance means nothing. Any individual can now theoretically have access to as much processing power as they would like and afford, and the dollar to MIPS ratio is falling like a stone. What does having those available CPUs translate into? One of the most interesting demonstrations of free-market

intelligence applications was the massively parallel cooperative process cryptanalysis of commercially available weakened cryptosystems. Communications plus massive processing gives a new twist to the idea of community memory--application of the experience, expertise, and brainpower (computer and human) inside a voluntarist community. This is similar to Vernor Vinge's example of a group of humans with a workstation being able to 'ace' any standard intelligence test. Computer supported cooperative work, or community processing, has been particularly potent with the cypherpunks--testing ciphers, designing remailers and chains, pointing out logical fallacies in government programs--they operate as an intelligence think-tank.

Other than such think-tanks or Helmer-Dalkey Delphi pools, the processing power available on the net, coupled with the informational resources (including NOSI) and community memory, has direct application towards non-intelligence community (IC) outcome forecasting, predictions of future trends, gazing into the crystal ball. Single-outcome (likelihood of a single potential outcome) assessments and binary solutions along Bayesian lines (iterative re-assessments given in probabilistic terms over time) can be quickly derived, and in fact constitute a noticeable fraction of the actual 'signal' content of the virtual communities. More interesting is the application to multiple spectrum-like predictive efforts; this forecasting technique allows far more accurate estimates, and maps well back to real-world situations. A continuum of a problem space is defined as a set of potential options that could be selected as 'game' turns; these options are mapped onto a linear space that expresses the relative degrees of some characteristic of the option space. Against this set of options are mapped the players involved with their potential alignment to an option based on past behavior, actual policies, stated positions, and likelihood of resource dedication to the problem; this provides a coherent mechanism to balance probability estimates of the actions of the players and potential outcomes. NOSI is particularly useful to research and tracking player profiles to map their behaviors and policies. What is striking isn't that this can be done, since IC agencies have operational programs doing such, but that the resources necessary are within the grasp of non-IC bodies. An example, quite relevant to the net, is the issue of cryptography. Options along a spectrum range from the left and 'all crypto is illegal' to right with 'strong crypto is freely available and open.' Many law enforcement agencies (LEAs) would fall on the far left of the graph, and as you move toward the right you encounter the financial community ('strong crypto for internal networks, weak crypto for consumers'), the general population ('confused, uncertain, reactive'), and so forth until you begin to hit the other end of the spectrum with cypherpunks ('strong crypto should be free, and we write the code for it') and crypto-anarchy ('strong crypto and privacy are historically inevitable'). Resource allocation is particularly telling--LEAs having access to the government coffers, lawmakers, policymakers, media, etc. and the cypherpunks have access to the processing power, community memory, and net. So far the positions have stalemated, but then again, nothing stands still. Events continually occur which effect the players and their positions, and change the balance of power; this is the strongest indicator that Bayesian iterative reassessment is essential, and actually maps the predictive graphing into three dimensions.

OPERATIONS

Espionage and operations are different concepts; as stated before, espionage is the use of illegal means to gain data for intelligence purposes. Operations in general tend to mean the use of illegal means for other purposes, although at times operations are not illegal, merely clandestine. The techniques used in espionage and operations are commonly referred to in the IC as 'tradecraft' and the net is a rich place for technique. The net is also a very useful place to mount conventional operations such as war, unconventional operations such as terrorism, and provide operational support across that spectrum.

TRADECRAFT

What is immediately attractive about the net is how it replaces certain older mechanisms in a fairly clean fashion--why risk using physical dead-drops, cut-outs, or forwards when you have available a number of mechanisms that can be made virtually risk free to the diligent operator? Remailers, remailer chains, and public-key cryptosystems such as Pretty Good Privacy (PGP) turn the net into an intelligence playground. An operator can blend in with millions of others and get an account with any one of hundreds of services, ranging from America Online (AOL) or Netcom to hometown mom-and-pop Internet service providers (ISPs), giving them electronic mail (e-mail), Usenet news, telnet, ftp, and world wide web (WWW) access. After downloading a copy of PGP and calculating a few keys, the operator can get an account on an anonymous remailer or the head-through-tail of a remailer chain. Messages can be exchanged between operational entities through the remailer chains, providing cut-out, forward, and drop services simultaneously. If proper selection of key sizes, remailer chains, and latency factors is made, no traffic analysis will penetrate the secure and authenticated message traffic. Messages can also be dropped through mailing lists, into newsgroups, left on ftp directories, buried through steganography in graphics files, faxed, or transferred in so many other ways it defies making a comprehensive list. Rational, thoughtful parties who do not break or violate tradecraft procedure need never worry about compromises to their communications, which opens the door for a number of additional techniques.

ORGANIZATION COMMAND & CONTROL

You can't be an organization without organization, or can you? The conventional view of organizations is that they revolve around a 'mission order' or intent; wisdom has it that this automatically implies a centralized coordination around the concept, with a hierarchical structure. Even spontaneous organizations play the game of 'follow the leader,' just like governments, armies, corporations, and clubs. The net changes things considerably, or at least provides a set of options that have rarely been tried. It is important to note that even though much of the net was built and intended as a support tool for the military, they have not taken advantage of the changes it allows and enables in the adherence of an organization to a mission or intent. Hierarchies make organizations function around commanders, where each step in the organizational pyramid act as the 'peripherals' or tools of the rank above it. Commanders need skills of leadership, originality, inventiveness, and increasingly honed skills of management of complexity. What changes in voluntarist groups (every member of the group agrees on the definitions and intent/mission of the group, unanimously) in the net is that they can accommodate as many commanders as they can get and form a heterarchy (authority is determined by knowledge or function, not position), or virtual nervous system for the organization.

Heterarchies satisfy a number of cybernetic principles:

- Principle of Maximal Autonomy, which defines the purpose of the net as a provider of tools for localized use rather than centralized control;
- Principle of Redundancy of Potential Command, which states that power and authority resides where information resides;
- Principle of the Subsidiary, which states that problems are best solved in the sub-system where they arise.

Interestingly enough, military organizations in tactical wartime situations reduce down to de facto heterarchies, but this is an unintended consequence, and becoming less the reality with the increasing power of centralized military C4I technology. Organizational configurations can be thought of with new metaphors 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 view all points as equal, with 'command' being an agreeable arbiter or mechanism to gain perspective (a strategic viewpoint as opposed to tactical). 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--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.' Organizations of this sort have enormous advantages in conducting intelligence work; they will tend to be small, are tightly directed, hard to detect, hard to stop, camouflage well, and the infosphere/information environment can accommodate any number 'inside' the same virtual territory.

RECRUITING

Operational organizations obviously require a high degree of security and trust; the cornerstone of such relationships is the proper selection of personnel. Mechanisms to attract 'like-minded' individuals are the foundation of the Internet--newsgroups, mailing lists, web pages, virtual realities. Weeding out of potential members through a thorough background investigation is possible as never before for non-IC or LEA organizations willing be operational for that purpose. Records such as phone, credit, banking, education, legal, travel, medical, and insurance are 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 subjects traffic. The reversal of this process is also important--'legends,' or manufactured personal histories, can be created and seeded across the relevant databases.

ARMAMENTS

The missing piece of the 'Table of Organization and Equipment' is armament, or weaponry. 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. Weapons don't have conflicts; conflicts are between people of will, those with a moral determination to change things. Subversion and conflict aren't 'bad'--without them, we would have perpetual status quo, stasis. 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 more important 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.

OPERATIONS & OPERATIONAL SUPPORT

Societies and cultures are founded upon and maintained by their 'social contract,' the terms and conditions that govern the relationships between members of the society; older, more complex societies have developed considerable infrastructure to support the elements of their social contract. The workings of the social contract and this supporting infrastructure can be termed a 'dependency infrastructure,' 'value chain,' or a number of other names, but the function is the same--to provide an economy of scale of function to support the level of complexity and specialization for the society. This dependency infrastructure is more and more essential to the functioning of a society as that society progresses from primitive levels to advanced technology; the most basic levels of the chain mimic the hunter-gatherer/agrarian stage of social development, and successive stages work to further insulate the advanced levels from the details of the previous stages. Dependency infrastructures closely parallel Maslow's Hierarchy of Needs--behavior is directed, but what drives that behavior? Basic dependencies are physiological (survival instinct, food, drink, health) and safety related (both physical and emotional, clothing, shelter, a feeling of protection); advanced dependencies, which manifest when basic dependencies can be fulfilled, include those of affection (family, a sense of belonging), esteem (self respect, achievement, appreciation), and self fulfillment (application of personal potential). Elements of the dependency infrastructure and social contract include executive and legal councils; civil services including macro and micro scale administration; social services such as education, healthcare, emergency services like police and fire departments; power systems, including electrical, fuel distribution; water and sanitation; transportation systems and maintenance, including motor vehicles and highways, trains, aircraft; financial mechanisms, such as banks, credit cards, equity markets; communication mechanisms, including telephone networks and media outlets; spiritual support; labor markets; legal and judicial bodies. What does all this have to do with conflict? Simply that all conflict--from conventional warfare to terrorism--has to do with selection and control of the social contract and dependency infrastructure. Control over a dependency infrastructure gives control over the leverage points of a political economy; damage to a dependency infrastructure can disrupt the economy of scale it provides, making the burden of the social structure too heavy to be self sustaining. Attrition warfare, waged for centuries and hitting a zenith with the American Civil War (19th Century) and World War I, sought victory through overwhelming or forcing a failure of the opponent's dependency infrastructure. Manoeuvre warfare, a more recent refinement, seeks victory through position or taking control of the key elements of the opponent's dependency infrastructure. Guerrilla warfare relies on making opportunistic attacks on the opponent's dependency infrastructure to make the moral and material costs of the conflict too great for the opposition to maintain. Political warfare seeks control of the society through the creation and manipulation of an alternative dependency infrastructure or social contract, commonly through the use of propaganda and psychological warfare. Terrorism is about actions directed against the opponent's dependency infrastructure and social contract intended to focus media attention in a certain way; terrorism as a form of war is commonly an adjunct to one of the other forms of warfare.

Thinking about warfare in terms of social contracts and dependency infrastructures allows a uniform method of considering conflict in general; this sort of conceptual model or 'cognitive artifact' is a force multiplier, a tool that makes any actions or operations potentially more effective in achieving the intent or mission. This is the most striking point of technology's impact on warfare--conceptual models and cognitive artifacts are becoming force multipliers, evolving the organizations to fight new forms of warfare using the models to augment operations, or play off a 'model to reality' arbitrage that raises intelligence and deception to a new plane (the fashioning of illusion to achieve real aims).

'CONVENTIONAL' WARFARE & THE FORCE MULTIPLIER

Technology and the mechanisms of the net have begun the transformation process of warfare– attrition warfare (direct physical occupation and control of the opponent) has turned in the direction of manoeuvre warfare (analysis of the opponent to discover dependencies and operations to leverage against those points). Look how the principles of war-making have been effected:

- Maintenance of objective; mission intent can be communicated to all operational parties to insure they can work within the framework established;
- Economy of force; intelligence and analysis can be used to 'right size' and meter the force used, or insure overwhelming force is used;
- Flexibility, Contingency; intelligence and communication tactically allows operational parties to react to changing situations and still remain inside the objective framework;
- Initiative, Tempo; the orient-observe-decide-act loop cycles considerably faster, and allows operational parties to continually make decisions and act on them;
- Manoeuvre, Leverage; intelligence and analysis have evolved to where dependency points can be identified and acted against;
- Ground is no longer a place to stand or move, but becomes a process, as embodied in calculations of physical tactical positioning, force multiplication/division, or conflict in an 'infosphere';
- Security, Deception; the rich technology and technique provide new levels of security, strategic and tactical;
- Simplicity; this point has a tendency to become lost in the wealth of options now available, usually in the direction of over-finesse;
- Entropy; accurate information negates entropy;
- Training, Readiness; the full gamut from education to operational simulation has been radically advanced; this is the most serious point of improvement;
- Mobility, Mass; technology has also radically improved this point, with miniaturization just being the beginning; a man with a laser targeting system, global positioning system, and communication system can be carrying only a few kilos of gear, yet have devastating firepower at his command.

Yet for all these advances, direct war operations are becoming few and far in between. It takes an advanced political economy to field this sort of force and afford the effort. Far more cost effective, other forms of warfare derive similar or greater benefits from technology and the net, and so they are becoming the primary mechanism for engaging in conflict.

OTHER FORMS OF CONFLICT AND WAR

Conflict arises internal to countries when there is dissatisfaction with the dependency infrastructure and social contract, or in expansionary conflicts, where one group attempts to impose their control over another group's dependency infrastructure or social contract. What the 'conventionals' call Low Intensity Conflict (LIC) are operations other than conventional warfare, an odd exclusionary definition. These can be operations to force failure of parts or the whole of a dependency infrastructure; or an insurgency, which is the creation and popular adoption of an alternative dependency infrastructure and social contract. A good example of this is the American Revolution (18th Century), which established a new social contract then fought to hold it. The adoption of an alternative dependency infrastructure or social contract is essential to establishing a viable revolution. This in fact is one of the strengths and reasons for success of the communist mechanisms for conflict--they supply an alternate, attractive, albeit unworkable social contract and dependency infrastructure that allows some continuity of control and stability for a society post-revolution. It also helps explain the nature of political Islam revolutions, which embody a social contract and infrastructural elements, in many ways antithetical to democratic or secular notions. These sorts of conflicts have rules of thumb the way conventional conflicts do, and find technology and the net just as useful.They have superior knowledge and intelligence; select the conflict setting and parameters (time, place, rules); know the territory; strict security and secrecy; sanctuary from detection or attack; have a focused core membership and imaginative leaders; be decentralized, establish no patterns; build a strong support base; wage psychological warfare. A detailed look at how the net augments this sort of warfare is instructive.

A ROADMAP TO POLITICAL WARFARE

Political warfare (polwar) strives to create an alternative social contract and dependency infrastructure and induce their popular adoption. This is commonly achieved through efforts of agitation, subversion, rioting, propaganda, psychological warfare operations, disinformation, diversionary diplomacy, economic manipulation and attacks, terror attacks, and guerrilla or paramilitary actions.

AGITATION, SUBVERSION, AND RIOTING

These are popular movements demonstrating overtly and covertly the rejection by members of the population of the 'prior' social contract and dependency infrastructure or elements thereof. Revolutionary movements need to build the support base of societal elements disaffected with the dominating social contract and dependency infrastructure. It is this core that establishes the alternate structure and acts as an example for potential new members and the society at large. The net is an ideal tool for management of this base members can be educated through the medium of the net; establish alternative structures for civil, police, and military matters; and organize events and initiate 'flash crowds' (spontaneous actions) designed to disrupt the existing social contract and attract recruits to the new contract. 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, DIVERSIONARY DIPLOMACY

Propaganda and psyops efforts have a ready tool in the net, as can be seen in how it affects some of the rules of thumb for such operations:

- Fix target and channel, use existing channels; the medium may or may not be the message, but the net does act as a considerable leverage point--the net is becoming a well defined entry point to the media cycle; once in the cycle, stories feed on themselves, and propagate through the more 'conventional' media outlets;

- Target pressure points; demographics on the net work highly in favor of targeted messages, providing numerous specialty forums with near-ideal spreads in income and age factors;

- Stress micro at the micro level, stress macro at all levels; the net is an international mechanism that can be used to manage local or topical messages, and with the same stroke of the pen, have wide distribution;

- Test messages and iteratively design them; while careful controls to limit distribution of test messages would need to be used, a 'natural selection' takes place that tends to kill messages that are non-viable, and propagate viable ones;

- Be flexible, run the operation in place; newcomers can't expect to manage propaganda efforts on the net, but once established inside of certain communities, operators can manage quite well;

- Know the context; the net is well structured to assimilate newcomers into the rules and nomenclature, providing a continuity of context that is quite striking;

- Set the tone properly, positive/prophylactic/negative; the net is designed to move information and it does so quite well; it also acts as a valuable forum to release information that is beneficial to the operation, acts informatively, or 'flames' the opposition;

- Timing, duration, and repetition of message are critical; the net has an extremely fast cycle of turn-over, but also has a way of rehashing topics and messages continually;

- Keep the content simple and emotional; this requires skill in construction of the content for the net, which tends to apply logic more than most media, but a direct message still cuts through the noise;

- Evoke group identifications; if managed in context, the net is a structured yet highly fractured social community; evocation of group identities is greatly situation dependent;

- Don't misstate facts, present alternative interpretations; this is already the mainstay of the net, like a dog worrying a bone;

- Establish trust; voluntary communities on the net are structured with de facto reputation markets, and past performance is a major factor in how a message is received and interpreted;

- Use no new issues, exploit existing ones; hijacking old topics and putting a new 'spin' on it is another favorite 'indoor sport' of the net;

- Aggregate the message; starting with the basic concept of any message and evolving it over time works well in the net, but only if the other rules are not violated (trust, context).

One of the 'problems' of the net from a psyops perspective is that many of the communities are already highly skeptical because of the education and experience of the individuals using the net. Disinformation tends to be harder to manage, but somehow always manages to find willing minds. Deception, the minor religion of the intelligence community and net alike, has an abundance of opportunities in the net, particularly the use of back-end active measures to damage perceptions of data or channels.

ECONOMIC INTELLIGENCE AND ATTACKS

The net offers a prime opportunity for exactly this sort of operation; money is mostly virtual, and there are endless opportunities. Operational groups can use economic intelligence and attacks for funding as well as the operational value of the mission. Without a 'political' objective, many of these operations are simply 'crime,' interpretations are irrelevant to considering their potential and application.

NET CRIMES

Net crimes are the functionality without the ideology:

- ‘cCrime' 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;
- Money laundering becomes greatly enhanced through the net, as does control of clandestine assets.

An example system for such transactions is easy to postulate; chained remailers with one remailer in the chain being the actual end-user, hiding dropped traffic with decoys to/from a public news posting pipe, all message traffic buried in a nested cryptosystem (two public key depths with 3DES/CBC and initialization vectors wrapping a message using a codebook managed by a pseudo-random number generator like Snefru). Such a system could be a secure bank, information store, dead-drop, cut-out, and forward; the only price to pay would be system support and processor time.

Dependency infrastructure and social contract elements maintained by systems connected to the net face attacks as well; these attacks are referred to as 'information warfare,' (infowar) and as much as I

dislike the term, I will use it here. Potentially effected infrastructural elements includetelephone 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 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 (DOS) 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. For example, one of the highest probabilities for such military infowar is the American Sixth Fleet (Middle East), which regularly services/repairs approximately 25 U.S. warships in Haifa, Israel. Along similar lines, all U.S. F-15 warplanes in Europe are serviced by Israel Aircraft Industries; Israeli development of infowar capabilities in their LAKAM group would make the potential for such an attack even greater.

Infowar is also more subtle attacks on the dependency infrastructure or value chain; misuse, perversion, or manipulation of data can be devastating in the right situation. Attacks along these lines have some distinct advantagesthey 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 net, and have an extremely high value in damaging the morale of the opponent.

There are 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. Infowar attacks use the net directly as the weapon, and this area of investigation is one of the most interesting possibilities provided by the introduction of the net.

INFORMATION WARFARE

Dependency infrastructure and social contract elements maintained by systems connected to the net face attacks as well; these attacks are referred to as 'information warfare,' (infowar) and as much as I dislike the term, I will use it here. Potentially effected infrastructural elements includetelephone 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 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 (DOS) 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. For example, one of the highest probabilities for such military infowar is the American Sixth Fleet (Middle East), which regularly services/repairs approximately 25 U.S. warships in Haifa, Israel. Along similar lines, all U.S. F-15 warplanes in Europe are serviced by Israel Aircraft Industries; Israeli development of infowar capabilities in their LAKAM group would make the potential for such an attack even greater. Infowar is also more subtle attacks on the dependency infrastructure or value chain; misuse, perversion, or manipulation of data can be devastating in the right situation. Attacks along these lines have some distinct advantages 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 net, and have an extremely high value in damaging the morale of the opponent. There are 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. Infowar attacks use the net directly as the weapon, and this area of investigation is one of the most interesting possibilities provided by the introduction of the net.

GUERRILLA WARFARE AND TERRORISM

Although the line between these two disciplines has 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, kidnapping, riots, hijacking; these tend toward civilian targets, usually directly on the assumptions and terms of the social contract. Terror attacks have evolved. 'First generation' terror efforts focused on an exhaustion strategy; targets were typically 'no retreat' hostage situations, which eventually were successfully counter-measured 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. The net can be used 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 IC and LEA sources. In short, the net is a ready tool for the hand of the guerrilla or terrorist, who will certainly wield it.

CONCLUSION

Is the net a viable intelligence tool? I believe I have skimmed the surface enough to demonstrate that it has significant value in tradecraft and operational support; it will also play an increasing role as the domain of operations with information warfare.

The 'players' of 'games' in the net can be anyone with access, more of whom there are every day; as with any tool that can become a weapon, all it takes is a man with the will to wield it as such. As the disparity between what can be accomplished using the net and the laws and covenants governing society fall farther and farther out of step, the potential for successful use of the net for intelligence purposes grows.

Can espionage on the net be limited? Certainly, with the adoption of freely available and commonly used strong cryptography. Common usage of cryptographic technology would turn the private signal content of the net into noise--one man's noise is another man's data, but only if you have the right key. Currently however, using the net for espionage is a valuable target of opportunity--better grab a pot because the sky is raining soup.

Can the effects of small and large scale criminal and infowar attacks be limited? While not as easy to solve, many things can be done:

- No system is secure, so don't rely on security to protect data; use strong cryptography. Strong cryptography can also protect against spoofing, viral attacks (authenticating all executable code prior to use), and many of the other ills of the net;

- Since break-ins and attacks are going to occur, systems need to be designed to accommodate 'safe failure,' including adequate controls on deletions of data (write-once optical drives, or hardware control of the write/erase functions of the storage), and common checkpointing (periodic back-up of stored data). Critical systems should have redundancy, and be prepared for the inevitable failure.

Can the operational utility of the net be limited? This is the 'ontological judo' of the Adversary--for the net to exist, it has to remain freely accessible, and as long as the net exists, ways will be found to move data from point 'a' to point 'b,' regardless of the controls. The net isn't the sort of place that can be 'occupied' in a military sense; it could be shut down, but nobody can 'take' the net

and hold or police it, and it will resist any such attempts. I'm not even sure it could be shut down at this point; the technology to re-establish it, even in a covert form, are wide-spread enough to make an 'official' shut-down improbable. Another point to remember is this--for an insurgency to work, there needs to be an alternative social contract and dependency infrastructure established. Consider the net--it already comprises such a system, and this is what makes it such a potent intelligence tool.

> *"...it is necessary for him to have a mind ready to turn itself accordingly as the winds and variations of fortune force it, yet, as I have said above, not to diverge from the good if he can avoid doing so, but, if compelled, then to know how to set about it." –Machiavelli, The Prince*

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, 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.