Michael Wilson

National Security and Infrastructural Warfare

I've been asked to discuss the complex, dynamic subject of national security. It's a curious selection of a topic for me, but perhaps not so curious–I'll be able to provide you with some perspective from the viewpoint of the professional opposition, given that the main body of my professional experience has been in operations and intelligence against sovereigns of one sort or another. What I'm going to attempt to do in the limited space I have is to give you an overview of the various opponents, and a few cognitive tools for understanding national security and conflict.

As a way of constraining the discussion, I'm going to use the framework of game theory: games and meta-games, players, strategy, tactics (action), and outcomes (payoff), all constrained within the pre-condition of the participants' will, intent, and objective. This is important to note, because not wanting to play the game (and national security is closer to being a game–or a joke–than most people wish to believe), or not having the will, leaves one with the worst game positions and outcomes (we have a word for pacifists–"losers"). I don't have the space or inclination to detail conventional game theory issues like the Prisoner's Dilemma or nuclear strategy games, but even a cursory attempt on the part of the reader will demonstrate the futility of an approach that ignores or avoids the game.

While we are all familiar with games from participation in them and as spectators, when it comes to national security, particularly vis a vis conflict, our understanding of games is flawed:

— constructed games are overly structured and polarized (win, lose);

— rule-making is generally not a function of the players, but some "superior" body; rules are aimed at the "level playing field," the "sporting challenge," and "balance" in the game;

— artificial constraints are imposed, such as time limits, edges (chess, field games), turns (horseshoes, nuclear weapons), rounds, hands, etc.;

— a "win" is defined, concretely, but varied across games, including point leads, gaining a position, capture of a piece, ranking or some other forms of order, "right" answers, and book solutions.

It takes great naiveté to even consider the real world on such terms: there are no restrictions, rules, or enforcement not of our own making; nothing is "fair," be they markets, competition, or "equal" players, "symmetry" doesn't exist, particularly in conflict; there is no such thing as a "win," and even "lose" is fuzzy (movements love having a martyr).

I've personally laboured a great deal in my own professional work attempting to construct and maintain a coherent model for understanding conflict and national security; while moving from conflict to conflict, sometimes in a primitive setting, other times in the most modern metropolis, I've always had to maintain my effectiveness–selecting an appropriate set of strategies and tactics and successfully carrying them out. I've noticed other professionals unable to cope: playing the wrong game; using inaccurate mental models with poor representations of the context and parameters, miscontextualization; a poor understanding of

risk, uncertainty, and arbitrage; an inability to context shift or engage in the "meta-conflict" spread across many continuous games in many contexts.

Infrastructural warfare (which I shorthand as "iwar") is my formalization of the cognitive tools that give me my "competitive edge"; iwar is a meta-system for conceptualizing conflicts/games by the targeted infrastructural dependency:

— attrition warfare forces the failure of an opponent by inflicting enough casualties and environmental damage to overwhelm the supporting infrastructure which makes the political economy function; this includes weapons of mass destruction, which cause the disruption of all dependent systems inside the target radius;

— manoeuvre warfare aims for control of the points of dependency in the military and political hierarchy/control structures through metered force or threat thereof;

— guerrilla warfare is the use of opportunistic force upon military and political dependency infrastructures such as command,

communications, and logistics, making the moral and material costs of conflict too great for the opposition to maintain; terrorism: is also opportunistic force, but focused on the social contract/dependency infrastructure, forcing a failure of social systems through an erosion of trust;

— propaganda operations direct against the growing human dependency upon observational proxies (media, including formal and informal, from conventional outlets to the Internet) in organized societies;

— political warfare (polwar) aims for control of society through the creation/manipulation of alternative dependency infrastructures or social contracts, commonly through the use of propaganda and psychological warfare;

— psychological warfare (psyops) operations aim to subvert/pervert/deny the information/communication tools that are a dependency of any organized system;

— information warfare (infowar) is a sub-class using attacks/denial of the specialized dependency infrastructure–the information infrastructure, or infostructure.

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 itself a force multiplier, making any actions or operations more appropriate and effective in achieving the intent/mission, regardless of context or context shifts (games and meta-games).

Players: State, Opposition

A State is conventionally described by its border, the arbitrary transition from one State to the next, the boundary of defense, one of the constraints on the scope of State control. The geographic definition of a State and the physical threshold point where national security is an issue has faded over time, as the need for "ground" as a representation of wealth, a means of production, has faded. National security, State power, and politics are interconnected and

defined by who owns and controls the infrastructure of the political economy (dependency infrastructures), the requirements/necessities of keeping an organized system functioning. These infrastructures find their origins in A.H. Maslow's Hierarchy of Needs, the ranking, in order of importance, of a person's needs that direct/motivate behavior and require fulfillment: physiological needs (survival oriented); safety needs; affection needs; esteem needs; and self-fulfillment needs.

Political economies/societies are defined by the developmental level of the infrastructures: a "primitive" society is agriculturally oriented; more advanced societies, the "developing" world, are industrially oriented; and the "modern" societies are technological. Each step in the evolution reduces the importance of the previous stage, but does not obviate it; advance from one stage to the next, more advanced stage is not through a simple, single advance, but an aggregation of a number of advances–tools, processes, and knowledge that lead to more complex tools, processes, and knowledge, all continually becoming ever more complex. Such infrastructures are rarely designed for their function, that of providing an economy of scale, but have grown like organic structures over time; complexity, however, forces specialization, and the material infrastructures and information infrastructures of the political economy "differentiate out" into more explicit systems:

— value chains (economic structures, like manufacturing networks, or services that provide Maslow's Hierarchy–food, water, fuel, power, travel/transport, markets, education, spiritual);

— social contracts (political systems, with written agreements (Declaration of Independence, the Constitution and Bill of Rights) and unwritten (a Victorian "code of behaviour"));

— infostructures (Internet, communication "transport" layers/networks);

— an information environment (media, a "community memory," the "signal environment").

Just as the level of development of a dependency infrastructure defines the sort of political economy a State possesses, the degree of State ownership and control defines the social contract and politics of the system:

— democracy makes provision for the greatest level of individual ownership for the average citizen;

— socialist/communist forms of government have ownership reserved to the "collective," which has rather dramatically been shown to lead to a tragedy of the commons–when everyone owns something, nobody "owns" it in a sense of being responsible for it, and thus the sorry state of economic affairs in such systems;

— fascist dictatorships/monarchies reserve ownership to "special" individuals, creating a clearly recognizable stratification in ownership, a two-tier system of Haves and Have Nots, with no free mechanism to rise from the Have Nots.

Categorization along these lines takes into account most of the elements of the dependency infrastructure, except for the element of the social contract, and this is where things get blurred. By definition, there will be powers reserved to the State, areas where the State holds monopoly control, hierarchical sway, or which it requires dependence upon from its citizens. Chiefly, these elements are money, defense, and the trinity of law/order/justice, all generally subsumed under the State's possession of a monopoly of force; Mao's "all political power

originates from the barrel of a gun" is largely correct–any attempt to dispute the power of the State in these matters will generally lead to arrest and imprisonment, or if resisted, State use of force (including lethal force). Citizens of a State may have some small role–service in the military (perhaps not conscription or mandatory service, but regardless, once in, the order of the day is obedience to the command hierarchy), a small voice in shaping law, participation in justice through jury service. By and large, however, States are consumers, absorbing a varying percentage of the resources of the political economy, and even the best of political systems erodes with time–a hegemony lacking diversity, increasingly unified authority leading to bureaucracy, where the worst draw down the rest.

This was why I framed iwar in terms of dependency infrastructure–not only is infrastructure the means necessary to wage war, but it is the prize to be won. Dependence, however, is equated with vulnerability, particularly where hierarchical or monopolistic structures of a State are concerned, and that dependency cuts both ways–into national security, and the security of the citizens. The State, as a consumer, and dependent on the function and output of the infrastructures of the political economy, is vulnerable to attacks, loss of function, and loss of economy of scale in the myriad networks which comprise the dependency infrastructure; safety, security, and control of dependent elements may not even be possible: by agreement with the citizens under the social contract, or because of cascade dependencies–a key dependency with its own dependencies outside the direct sphere of State control (petroleum and "strategic" minerals being easily recognized examples). This is the primary reason for the "creeping definition" of national security into "national interest," which crosses boundaries and borders–in a world where the more advanced, complex markets, goods, and services are constructed from webs of interconnected resources, material and human, where do you draw the line? Threats to national security and national power get muddled together: dependency and monopoly play off against diversity and redundancy, based on the context and which side you're on (e.g. Microsoft's stranglehold on the operating system market is simultaneously an extension of U.S. power across the world, and one of the greatest security threats to the U.S. infostructure). The citizens, of course, get screwed; by the State reserving monopoly or hierarchical control of certain elements, the vulnerability of those elements adversely impacts on the people theoretically served by the State: attacks on currency and financial systems; centralized defense systems that are now visibly lacking when required to address modern and future threats; extended definitions of national security and national interest that actually increase the need for various costly distant interventions (military, financial, political), creating a geopolitical "double bind," simultaneously the required global policeman, and being reviled for it (where reprisals take the form of attacks on the citizens, not those responsible for the decisions). Control the context and you control those dependent within it; attack the context, and you attack those trapped within it.

Opposition (internal) and threats (external) to national security are, at this point in history, impossible to categorize easily; repressive regimes spawn resistance from within and without, as surprisingly do ostensibly open, free democratic States. Internal opposition and resistance are the problems the State creates itself; regardless of the process of decision making in the social contract, there are always going to be a percentage pleased with the way things go, and a percentage which feels disenfranchised, unhappy, or oppressed–and these small percentages are increasingly willing and able to "do something about it." Seemingly with every decision, and there are more decisions made in democracies than in more authoritarian systems, a society is schizogenetic–splitting up into opposition groups for civil disobedience, paramilitary activity, guerrilla actions, terrorist attacks, or other "criminal" activities. It doesn't matter if the motivation is political (whether a new system, or the "we want to have our turn" brand of political control), pathological, or profit, the capacity to challenge the

system has devolved to the level of the individual–deviancy defined down. External threats are far more simple to cope with, at least cognitively–they're bigger, slower, and easier to identify, analogous to early mammals coping with dinosaurs. Conflicts between States generally make "more sense"–money, land, control, power, prestige, and/or punishment are common, well-understood motives. States themselves play dependency games–sanctions, controlled technology, "gift" aid, development packages, technical assistance (particularly in "threat" technologies such as nuclear/chemical/biological programmes of dual/mixed use, space technology, materials and manufacturing processes, etc.), all designed to provide the benefits of progress, but without the know-how or control. Such activity to control the game by controlling the players rarely works–information defies controls, "puppet" States or allies extend the national security/interest boundary into increasingly risky contexts, and some States have mastered a "submit and rule" strategy that has reversed the dependency-control relationship (e.g. Japan, Saudi Arabia, Israel). Clearly, strategy is poorly understood.

Strategy in the Game of National Security

The single most significant flaw in national security strategy is thinking in constrained games terms, particularly the polarized win/lose. Understanding any game that models real world situations requires the addition of two new strategic positions–Not Lose (NL) and Not Let Them Win (NLTW). The strategies need a few words of explanation, and they are actually nested concepts (in the order presented):

— lose, which means generally that you're dead (unable to play), or unable to control, which amounts to the same thing; note that being dead might disadvantage your play, but could serve some benefit to others playing in the game (martyr tactics);

— not lose, which is just what it sounds like–the primary goal is to stay alive, because the dead don't get to play, but after that, there are no rules; this sort of player forms the core cadre of any movement, and is voluntarist, inexorable;

— not let them win, which comes after survival and playing the game, means that you will do anything to deny an opponent a win, you'll make it cost them to play in the game at all, and they'll only control what they stand on;

— win, which means you control the ground, define the rules, and frame the context; for what it's worth, there's no such thing as a win in the real world.

Some examples are necessary, and they'll explain the expanded strategies fairly well:

— World War II, viewed as one game, was played for win/lose (note that playing for a win in a polarized game is zero-sum; if you don't win, you're going to lose, trite as that may sound); interestingly enough, if you view WWII as only a game nested in a meta-game, Japan and Germany, who had to unconditionally surrender, shifted their strategic positions to NL shortly after the war and as the Cold War started, much to their benefit;

— the Cold War, the struggle in the latter half of the 20th century for political dominance between collectivism and (arguable) individualism, was a meta-game; it shifted contexts, rules, playing fields, players, strategies, and just about any other dynamic parameter during the course of the conflict–you can't look at an isolated game and make any real sense out of it without relating it back to the meta-game;

— World War I, incidentally, was where you can see two exceptional individuals who epitomized the NL and NLTW positions; NL was demonstrated by Paul von Lettow-Vorbeck in the battle for German East Africa, who, from 1914-1918 waged a guerrilla war which held the attention of between 10-20 times as many of the opposition as he had men in his command; he remained undefeated until German surrender in Europe and orders to cease hostilities stopped his effort to create as much chaos and draw as much attention as he could, always moving, always inflicting damage, never defeated (and at the cost of millions of pounds to the British); the NLTW position was used well by Thomas Edward Lawrence, also from 1914 to 1918, in his participation in the Arab Revolt in the Middle East against the Ottoman Empire; Lawrence's strategy is summed up simply–while his opponent could strengthen any one point against his ability to attack, he couldn't strengthen every point against him; Lawrence used mobile guerrilla attacks to keep the Ottoman Empire from being secure, and the cost of the Hashemite revolt eventually collapsed the Turkish front in favour of the Allies; Lettow-Vorbeck and Lawrence are icons which led to subsequent development of special operations groups worldwide; I cannot do either of them justice, so I can merely recommend that you find the histories they've left behind and read them;

— Mutually Assured Destruction (MAD) was a strategy of the Cold War nuclear era; playing to win meant you had to launch your missiles, while deciding not to play would guarantee a lose; playing the game at least put you in an NL position, and MAD was an instance of NLTW–the ballistic-missile equipped submarine fleet would always have a retributive strike capability; an interesting artifact of the period was the NL strategy known as the "trigger deterrent"–European States feared the use of tactical nucs in the European Theatre of Operations (ETO), and let NATO command know that use of tactical nucs in the ETO would prompt a launch of a long-range nuclear missile at either the U.S. or U.S.S.R. (irrelevant which), triggering their MAD retributive strikes, and thus spreading the misery around; if Europe was going to be devastated, they were going to take the superpower players with them;

— the Viet Nam conflict shows the nesting of NL, NLTW, and win–the core cadre of the Viet Cong and North Vietnamese Army waging a continual, regular guerrilla war, with a huge, dynamic support network among the increasingly disillusioned or injured "civilian" population; an NL strategy keeps the core movement alive, regardless of losses, providing an anchor to add additional resources and expand into a more materially costly NLTW strategy, and eventually collapsing the U.S. will to play the game; this process chain (NL, expanding to NLTW, to win), combined with some proposed political economic structure (such as a new, alternative social contract), has long been the key to guerrilla movements (see Mao's "little red book" or Guevara for the collectivist version);

— the Gulf War (Desert Storm) showed examples of all the strategies; the U.S. playing to win, Iraq vs. Kuwait playing win/lose, Iraq vs. the U.S. chose to play an NL strategy (which is why Hussein still controls Iraq), the Arab Coalition the U.S. put together against Iraq playing a NLTW strategy; had Saddam Hussein played win/lose with the U.S., things may have been very different, but the U.S. and Iraq were playing different games–and any assessment of the aftermath of the conflict has to say that for all the impressive performance of U.S. miliary forces, they didn't win, because they weren't playing the same game as their opponent, who deflected the impact through his NL strategy, which has translated into a practical win inside Iraq;

— a word on why there is no practical win is worth mentioning: did Israel "win" occupied Palestine, do they have peace? Did Great Britain "win" in Ireland? Resistance strategies

become much more understandable with the new positions in mind. No wonder people are nostalgic for WWII–viewed as a stand-alone game it was a "good fight," but it takes a deliberately short-sighted view to see it that way.

Tactics/Actions in the National Security Game

The tool I use to think about conflict, iwar, takes advantage of and targets frailties, shortcomings, and defects that have occurred as society evolved; it can be waged any time, any place, against any culture, and under any circumstance, since even the most primitive of societies has infrastructure (by definition), and dependency is so much the prevailing circumstance that it has become almost unnoticed.

Any tactics attacking or subverting the national security of the State need to "attack-in-depth" using a combination of approaches:

Denial Of Service Attacks (DOS)

—Attacks which deny society or a subsection of society access to, utilization of, or benefit from infrastructure in whole or part; for the material infrastructure, DOS-M attacks, attacks on infostructure, DOS-V (for "virtual" infrastructure);

— DOS-M attacks vary from blowing up bridges or communication switching centers (more advanced societies) to mass attrition attacks on civilian populations (in societies where people are the infrastructure, such as agrarian-oriented economies);

— DOS-V attacks ("information warfare," "netwar," or "cyberwar") can be hackers shutting down traffic control, attacking software controlling telecommunications switching, or mass flooding of networks which manage social processes, attack tools vary from live "cracking" of systems to automated attacks with computer viruses or network-packet flooders;

— The intent of iwar is effectiveness in attack, and the method of denial will vary with circumstance; regardless of specifics, iwarring in this fashion upon a target is intended to force failure in a process, or control/automation of that process.

PsyWar Attacks

— Rather than outright (and not terribly subtle) destruction/denial of infra/infostructure, subversion/perversion attacks target processes (material, virtual, or human) and decision processes (thus degrading options or recommendations they provide); or impair/damage models, where errors cascade and propagate throughout models, not always in obvious ways;

— Psychological warfare attacks (psywar) are more difficult to accomplish than DOS attacks–it requires a human touch to debase human decisions; however, modern society has real-time demands for immediacy, which increasingly force automation of decisions, placing human judgment secondary or out of the loop entirely, trusting in machine data and operation in real-time;

— These dependencies are dynamic and have thresholds–alteration of a medical record to change a blood type doesn't impact the individual until that information becomes critical to making an accurate decision; this means such attacks can occur on systems or information

while it's unprotected because at the time of an attack, they seem unimportant or inessential, an incorrect assumption.

PolWar Attacks

— Political warfare is propaganda, disinformation, agitation, and social subversion, a specific subclass of psywar where subversion is directed at political processes, a case of ìpolitics by other meansî;

— As I mentioned before, one of the keys to making changes in society or political economy is to create and provide an alternative social contract, gaining adherents through persuasion or compulsion, or by "forcing the hand" of the existing structure into making reactive changes; the modern infostructure provides numerous mechanisms for the creation, support, and proselytization of "intentional" communities; the technological tools and communication channels provide unparalleled mechanisms for the creation and dissemination of propaganda and disinformation, to organize groups, coordinate actions, and otherwise subvert the stability of social structures.

Conclusion: Outcomes, Payoffs

As you may have noticed, my perspective, and the iwar "meta-game" toolset, are about national insecurity and destabilization; the new game positions of Not Lose and Not Let Them Win are important to understand because iwar will not provide a "win," it will not provide control to a player even when successful. The iwar strategies and tactics are about collaterally backstopping other operations–offensive, such as some pre-emptive attacks, but only as part of a supporting/combined operations attack-in-depth, or a coercive effort; or defensive, such as denial or retributive attacks. Offensively, pre-emptive attacks like the mythical Electronic Pearl Harbor would be as fruitless and counter-productive as the original Pearl Harbor was; iwar attacks can, have, and will inflict chaos on an opponent (such as psywar attacks on tax bases, economic key points, currency, markets, and the information environment). Denial of something such as the Global Positioning System (GPS) in future conflicts will be a significant tactic, but even denying GPS only reduces the offensive ability of the opponent, it doesn't put them out of the game. Rome wasn't built in a day, and it doesn't fall in one either; proponents of infowar "sudden death" attacks are dreaming of cheap, simple, and totally unrealistic victories. Real victories come from long, slow, subtle subversive efforts, and even here, forewarned is forearmed–a wily opponent could shift strategies from win/lose to fallback positions of NL and NLTW, keeping the game going for decades, centuries, or millennia if necessary, until the game can be turned around. Being smart about strategy–knowing when to use NL and NLTW as positions–and knowing the iwar cognitive toolset, will go a long way toward helping you understand national (in)security and conflict. Hell, it might even put you in the game.