Threat Kingdom

Lieutenant Colonel Bill Flynt, US Army

In Greek mythology the gods sometimes punished man by fulfilling his wishes too completely.
— Henry Kissinger

Mr. Gorbachev, tear down this wall.
— Ronald Reagan

WE GOT WHAT WE ASKED FOR. Now we need to adapt.

Futures Industry Association

***Kennan's world assumed the intent of specific state actors based on their public declarations and other information. Determining others' capabilities—for example, by counting missile silos—was essential.* In today's security environment it is capability that must be assumed.**

In a classic article on threat perception written early in the Cold War, J. David Singer defined a threat as a capability coupled with intent.[1] He explicitly defined a term he thought was used too loosely in vital security debates at that critical time. His definition remains a basic point of instruction in security studies. Unfortunately, academia's precision has not improved the focus of US post-Cold War security policy. Contemporary security policies declare hunger, civil unrest and other conditions of the security environment as threats. Consequently, the term "threat"—expanded to mean almost everything—means little.

Singer's definition helped security policy planners focus on capabilities when they were measured in time of flight, throw weights and megatons of yield. The intent of the Soviet Union was assumed within models of massive retaliation, deterrence and mutual assured destruction. A key objective of the Cold War's intelligence effort was finding out whether capabilities enabled that intent to become a threat, and if so, how great of a threat. In retrospect, it was a simpler time.

Many things have changed. For instance, despite great effort to describe the current security environment, no recent articulation of US national security strategy equals the coherent vision of former US State Department Chargé George Kennan for containing the Soviet Union.[2] It may be too much to expect a similarly elegant vision for protecting US interests in the contemporary security environment. Kennan's world was less complex than the security environment confronting today's strategists. Likely there will be no neat, concise statement of national strategy directing the means and ends of the United States over a long period. Kennan's world was the aberration and his lack of confidence "in the ability of men to define hypothetically in any useful way, by means of general and legal phraseology, future situations which no one [can] really imagine or envisage" may better define our times than his.[3]

In today's increasingly complex security environment, states are not the only major actors, and technology arms small groups with weapons that in the past were held only by great powers. Technology and the proliferation of knowledge have made biological, radiological, chemical and cyber capabilities available to nonstate actors. Kennan's world assumed the intent of specific state actors based on their public declarations and other information. Determining others' capabilities—for example, by counting missile silos—was essential. *In today's security environment it is capability that must be assumed.*

Past conventional wisdom that an actor's intent could not be known exaggerated the difficulty because counting missile silos or armored formations was an easier and obvious alternative. In fact, an actor's intent can be known, but it requires much more than counting silos. Unfortunately, given the existing capability of dozens of actors, state and nonstate, to strike America's critical infrastructure and population with weapons that cannot be counted from space, determining intent is the only remaining option to identify threats.

Watching Them Watch Us

The appearance of weapons of new concepts, and particularly new concepts of weapons, has gradually blurred the face of war.[4]

— Qiao Liang and Wang Xiangsui

Crafting an effective security policy requires understanding three elements: self, environment and threat (see Figure 1). Understanding self means knowing the ends desired, capabilities possessed, resources available, acceptable courses of action and other aspects. The environment interactively affects both self and threat and can be modeled using core assumptions about its characteristics.[5] For example, a common model of the security environment assumes that states are the primary actors; the system is self-help without an overarching authority to referee disputes; survival is the ultimate end; and power, whether measured in terms of economic, military or other instruments, determines rank in the system.[6] The requirements for knowing oneself and the environment have changed relatively little. Understanding threats, however, has become more difficult.

Key US security officials have documented the capability among dozens of states and other actors to strike the US population and critical infrastructure with a variety of means.[7] The Cold War environment of clear intentions but unknown capabilities has changed to one of given capabilities, but unclear intentions. The means of striking the US population and critical infrastructure are no longer limited to strategic nuclear delivery systems but now include laptops and even smuggled chemical, biological, nuclear and radiological (CBNR) agents delivered by unwitting commercial carriers on time, on target. Attempting to identify threats based on capabilities has lost some measure of relevance when so many possess the requisite capabilities. Tracking programs for weapons of mass destruction (WMD) is important but increasingly difficult and still does not actually confirm threats. Since trying to track capabilities is nearly futile in a security environment where capabilities are both easily concealed and proliferating rapidly, assessing intent has become increasingly important.

The means of striking the US population and critical infrastructure are no longer limited to strategic nuclear delivery systems but now include laptops and even smuggled chemical, biological, nuclear and radiological agents delivered by unwitting commercial carriers on time, on target.

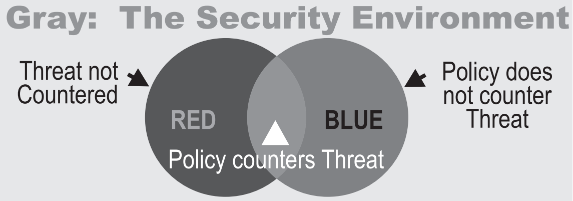

Gray: The Security Environment
Threat not Countered
Policy does not counter Threat
RED
BLUE
Policy counters Threat

Figure 1. Seeing Red, Gray, and Blue
(Understanding Threat, Environment, and Self)

A common concern is that assessing intent is like mind reading—other actors are opaque entities that may be neutral, friendly or hostile. However, such opaque actors are abstractions found in formal theory's black boxes. Adopting the mistaken belief that intent is unknowable leads one to view another actor as a strange dog encountered on a random walk: will it wag its tail, move along or go for the throat? One knows its capabilities but not its intent. However, usually a great deal is, or could be, known about other actors, particularly states. States' interests, decision-making structure, institutions, track record and key personalities are known with few exceptions. Additionally, states are not opaque to analysis. Bureaucrats, diplomats, military officers, journalists and others can communicate policy directions and provide insight into likely actions. Similarly, nonstate actors also can be analyzed for insight into their future actions. Intelligence agencies have many tools to gain insight into an actor's intent. One of the newest is the mining of text or data about the actor.

During the Cold War information was more restricted than it is today. Two fundamentals have changed. First, the collapse of the Soviet empire loosed many forces, perhaps the most potent being millions of minds and their voices. The second factor contributing to the information explosion is technology. Freedom of the press worldwide increases information flow as does globalization of television and the exponential growth of the Internet. Ironically, the vastly increased information available has not produced better insight. For instance, during the Cold War a public pronouncement by a Soviet official could be relied upon to reflect an official line. Whether it was disinformation or not, they knew we were studying the statement, and we knew they knew. The relative scarcity of information on certain topics made messages about these topics important to study, regardless of accuracy.

One would like to know what potential opponents are thinking. Adolf Hitler's *Mein Kampf* suggests that sometimes threats really do reveal their intent. Some intelligence tools like satellite reconnaissance have limited utility to determine intent, especially when capabilities such as cutting-edge WMD development programs are the target. Likewise, electronic eavesdropping may be deaf to encrypted communications over fiber-optic networks. These collection approaches have the challenge of obtaining and sorting data. However, a new approach exploits the twin expansions of freedom and technology and can mitigate the effectiveness of technological countermeasures safeguarding threat information, as well as distinguish between data and noise. Protecting all information is impossible, and the expansion of information available increases the probability that important data, even if only in partial form, lies outside protected systems where data- and text-mining technologies can provide qualitative analysis.

Liang and Xiangsui stated "A single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons."

Text mining means processing a document through an information-sifting tool. Text-mining tools vary but generally they identify the language of a document, summarize and categorize a document, extract key words, proper names and multiword phrases, report frequency of word and phrase occurrence, statistically rank a document's relevance to a specific topic and glean other information. Some incorporate a web-crawling capability, extract latitude and longitude data, depict information in spatial or temporal relationships, discover linkages or chains of related information, cluster records by like informational content, conduct cross tabulation analysis and include statistical packages. Advanced use of a text-mining tool involves programming the tool to sift a database for specific data and linkages. Text mining can process a huge volume of information, both real-time and archived and identify patterns that escape human analytical capability. Text mining is a powerful tool but not a panacea. The products require trained, human judgement to make them useful.

Any actor's security elites express thoughts that have been influenced by high-level intelligence, military and diplomatic briefings, interagency working groups tasked with policy formulation, blue-ribbon commission reports and other information-dense sources. Those thoughts therefore contain traces of distilled policy-formulation activity. Analysis of many sources may reveal patterns and linkages that trace the outlines of an actor's future policy and actions. The optimum level for targeting qualitative analysis is probably not the pinnacle of power, although that is necessary. Many statements by leaders are rigorously vetted through their staffs, including even their seemingly impromptu remarks, and by the time the leader publicly announces a policy it may be in motion. Depending on the actor, the richest information sources may be within the two or three concentric rings around the leader. These elite circles prepare the decision briefings, attend the interagency working group meetings and draft position papers that inform decision makers and shape policy.

From a security perspective we want to know who the threats are, the means they intend to use, their targets and the ends they are pursuing. This is fairly easy when dealing with an opposing state, overt conflict, known capabilities, targeting for optimum military effects and clear ends based on announced war aims. A greater challenge is understanding emerging threats in the current security environment such as actors (or states portraying actors) employing unconventional means against nontraditional targets, for widely varied ends through asymmetric, potentially anonymous, strategies.

This article examines a single book to demonstrate text mining's utility. For actual analysis a single source is insufficient; hundreds, if not thousands, of sources would be mined. But the example demonstrates the process. The publication is *Unrestricted Warfare* by Qio Liang and Wang Xiangsui, both senior colonels in the Chinese military. In their book, the authors detail a strategy for war against the United States that avoids strengths and attacks vulnerabilities. They argue that future war is not limited to the military domain and that conflict will encompass all human activities, including those traditionally viewed as nonmilitary and irrelevant to military outcomes. The credentials of the authors, the official publication of the book and the laudatory reception of their work suggest that their thoughts may help shape the general outline of emerging Chinese doctrine. The book even sketches some potential strategic outlines of attack should there be a conflict between China and the United States.[8]

A threat kingdom actor is the most dangerous potential opponent, able to engage across the entire conflict spectrum in time, space, intensity and instruments of power, including strategies of asymmetry and anonymity. The concept of a threat kingdom is not synonymous with the label of superpower or great power.

Text mining of *Unrestricted Warfare* followed a structured list of threats, means, targets and ends to classify passages. This structure functioned as the study's codebook, a listing of all terms used to identify elements of interest. The codebook was supported by a dictionary that defined what each code meant, gave the context appropriate for assigning a code to a passage, determined when the code would not be assigned to a passage and gave an example text passage corresponding to that specific code. For example, each text passage was analyzed, or mined, to reveal a specific actor by both capability and intent, the means the actor employed, target selection and the ends desired by the actor. Within each of these four categories the passage was further analyzed, with codes assigned to a specific type of threat, specific means, specific target types and specific ends sought as depicted in Figure 2.

Using the table's coding structure reveals patterns inherent in the text. Code chains, or logic linkages, consisting of Threat↦ Means↦ Target↦ Ends were clarified, such as Information Warfare Team↦ Cyberstrike↦ Banking and Finance↦ Asymmetric Conflict/Contain the United States. Additionally, the coding process allowed multiple coding within categories, which provides better resolution of intent. Recurring clusters of codes within a category, such as Cyberstrike/Economic Attack/Information Operations within Means suggest that these specific combinations of Means should be expected in future conflict with an actor whose data was mined.

Qualitative content analysis yields information and patterns within text (as quantitative content analysis does within numeric databases) that authors (database managers) themselves may not know is there. This powerful, automated tool can sift vast amounts of data, flagging the most promising for human analysts. Clarification of patterns, frequency of word or phrase occurrence and other tools help analysts see "red, blue and gray" perspectives and interrelationships, as illustrated in Figure 1. There are limits to what can be revealed by mining, and well-designed analysis integrates seasoned human judgment with mining tools. Common sense should be used in reviewing chains, patterns, clusters, frequency of occurrence and other results of qualitative analysis. Important in determining intent, qualitative analysis is a potent tool—but remains a limited weapon. To determine intent, or "see red," one must know what actors meant, not just what they said. Threats are looking at the United States. The United States should look at them to determine what they see.

Seeing Red

Proposing a new concept of weapons does not require relying on . . . technology, it just demands lucid and incisive thinking. However, this is not a strong point of the Americans, who are slaves to technology in their thinking.[9]

— Qiao Liang and Wang Xiangsui

There are many red perspectives. Known threats, such as specific states or nonstate actors, could be studied. Additionally, theoretical actor types, such as a pure-form transnational criminal organization, could also be analyzed for insights into that model's preferred means, targets and ends. Studying many red perspectives can help model a holistic typology of threats existing across the security environment, or a "threat kingdom." In this context, the definition of kingdom corresponds to the scientific use of the word as "the highest and most encompassing group" of the primary divisions into which objects are classified, such as the animal, mineral or plant kingdom.[10] Ordering threats in categories (analogous to the scientific ordering of kingdom, phylum, class, order and so on) enables better understanding of a specific threat's motives, means, methods and mission. A threat kingdom encompasses all possible capabilities and intents contained in the security environment.

Different red perspectives may overlap by threat type, probable means chosen, targeting preferences and ends. Some red perspectives may be unique. Actors may closely approximate a pure type, such as an autonomous terrorist organization, while others, such as China, may possess both the capabilities and intent to employ the total spectrum of different threat types in a potential conflict, and thus constitute a complete threat kingdom within a single actor.

In the example of *Unrestricted Warfare*, the authors believe that open conflict between conventional forces arrayed against each other in formations is obsolete.[11] Conflict, especially against the United States' currently preponderant military power, will not conform to past models such as the Gulf War. Their argument is supported by conventional military wisdom: an intelligent actor "avoids strength and strikes weakness."[12] They state that the overwhelming success of the US-led multinational forces and the emergence of new weapons have paradoxically sounded the death knell of such conflict. Instead, conflict "using all means, including armed force or nonarmed force, military and nonmilitary, and lethal and nonlethal means to compel the enemy to accept one's interests" is the new face of war.[13] The authors reason that confronting the United States militarily is futile and unnecessary since new means of attack expand the types of targets.

The banking and finance system is a component of critical infrastructure, but like the emphasis on cyberstrikes as a subcomponent of information operations, the heavy emphasis on targeting the US banking and finance system by this particular red perspective makes it necessary to track it with a unique code.

Technology has created "weapons of new concepts."[14] These new weapons are more lethal than past weapons. But developing them is futile in today's security environment. The development of improved weapons is expensive, America already has a decided lead, and these weapons do not escape the constraints of the Gulf War-style combat. A breakout strategy called "new concepts of weapons" is required to successfully prosecute war in the current security environment, especially against the United States.[15] This red perspective "views as weapons all means which transcend the military realm but which can still be used in combat operations . . . everything that can benefit mankind can also harm him . . . there is nothing in the world today that cannot become a weapon . . . breakthrough in our thinking can open up the domain of the weapon kingdom at one stroke. As we see it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons."[16]

Explicit in the argument is the expansion of targets. Classic warfare was directed against armed forces. Liang and Xiangsui argue that civilian populations will bear the brunt of future war due to countervalue targeting.[17] "What must be made clear is that the new concept of weapons is in the process of creating weapons that are closely linked to the lives of the common people. Let us assume that the first thing we say is: The appearance of new-concept weapons will definitely elevate future warfare to a level which is hard for the common people—or even military ones—to imagine. Then the second thing we have to say should be: The new concept of weapons will cause ordinary people and military men alike to be greatly astonished at the fact that commonplace things that are close to them can also become weapons with which to engage in war. We believe that some morning people will awake to discover with surprise that quite a few gentle and kind things have begun to have offensive and lethal characteristics."[18]

This red perspective's explicit advocacy of targeting and denying critical infrastructure systems may be a harbinger of warfare to come. Electricity, water, national financial systems, transportation, public health, emergency services and telecommunications are examples of targets that could be affected by new concept weapons. This strategy avoids US strength, targets weakness and transcends constraints of a classic military perspective. However, the target set is not limited to physical facilities. Qualitative content analysis reveals, for example, that the authors include "gene weapons" in their arsenal of new concept weapons.[19] Genetic weaponry engages living organisms, such as crops, livestock and human populations. Given the embryonic stage of genetic research and the widely publicized failures of genetic medicine in human subjects to date, research and development of gene weapons may promise a chilling future of unintended consequences.[20]

The Threat Kingdom

> *The new principles of war are no longer "using armed force to compel the enemy to submit to one's will," but rather are "using all means...to compel the enemy to accept one's interests."*[21]
>
> — Qiao Liang and Wang Xiangsui

A pure threat actor is less complex in capabilities and intent than a mixed type. The most complex actor would possess "the highest and most encompassing" capabilities and intent and comprise a threat kingdom of potential strategies. A threat kingdom actor is the most dangerous potential opponent, able to engage across the entire conflict spectrum in time, space, intensity and instruments of power, including strategies of asymmetry and anonymity.

The concept of a threat kingdom is not synonymous with the label of superpower or great power. Superpowers and great powers may be constrained by a variety of factors including norms and political institutions. The United States, while a superpower, does not embrace assassination as a legitimate use of force. Britain, while a great power, does not

Figure 2: **Emerging Threats, Means, Targets and Ends**

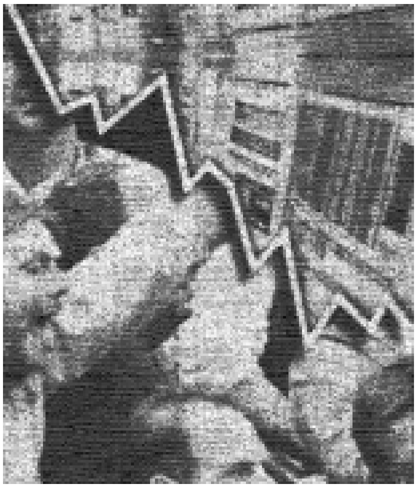
Threats	Means	Targets	Ends
Autonomous Terrorist Organization	Assassination	Banking and Finance †	Asymmetric Conflict ‡
Cult	Biological Agent	Biological Research/Production/ Storage Installations	Contain the United States
Economic Warfare Team	Bomb	Business	Economic Advantage
Fringe Group	Chemical Agent	Chemical Research/Production/ Storage Installations	Expand Power
Hacker	Cyberstrike	Continuity of Government †	Financial Gain
Information Warfare Team	Direct Action	Diplomatic Target	Hate
Lone Wolf	Espionage	Electric Power System †	Ideology
Paramilitary Group	Extortion	Emergency Services System †	Metaphysical
Spy	Hoax	Water System †	National Security Advantage
State Sponsored Terrorism	Information Operations	Government Installations	Political Change
Traitor	Nuclear Weapon	Law Enforcement	Political Influence
Transnational Criminal Organization	Radiological Agent	Military Installations	Revenge
State *	Economic Attack *	Nuclear Research/Production/ Storage Installations	Survival
Transnational Actor *	Genetic Agent *	Oil and Gas System †	Vandalism
		US Population	Obtain WMD
		Public Health System †	
		Telecommunications/ Information System †	
		Transportation System †	

* During text mining it became clear that this particular red threat perspective envisioned two threat types and two means not templated in the analysis design. State and Transnational Actors: In context, State should be understood as the primary actor portraying another actor, as was anticipated with the threat code "State Sponsored Terrorism." In context, Transnational Actor spans a broader universe. It can be understood as a well-known institutional actor, such as the International Monetary Fund or as a private corporation for instance, the Private Military Company (PMC) Sandline, Inc., a globally operating military-services organization. The means Economic Attack and Genetic Agent were cited by the source document and added to the typology. Economic Attack involves a number of methods from trade sanctions to commodity dumping. Genetic Agent is a pathogen designed to alter genetic material in crops, livestock or humans.

† These codes collectively compose the US Critical Infrastructure, as defined by *Presidential Decision Directive 63*, 22 May 1998.

‡ Asymmetric Conflict was coded for passages detailing it as a core characteristic. Asymmetric Conflict is not an end in itself, and when it occurred it was coupled with an end code to specify the threat's objective.

pursue genetically altered bioweapons. Here again is the importance of distinguishing capability and intent in assessing threat. Many actors have the technical knowledge to develop and employ all capabilities, but most do not intend to do so. It follows that a superpower is not the most dangerous opponent an actor in the current security environment can face; a threat kingdom actor is the most dangerous opponent.



Waging what this red perspective refers to as unrestricted warfare depends on two prerequisites: first, a complete toolbox of capabilities and second, the intent to use them if justified by the ends. "This kind of war means that all means will be in readiness, that information will be omnipresent and the battlefield will be everywhere. It means that all weapons and technology can be superimposed at will; it means that all boundaries lying between the two worlds of war and nonwar, of military and nonmilitary, will be totally destroyed."[22]

The most common chain in the form of Threat↦Means↦Target↦End cited by the Chinese strategists reveals a pattern of State↦Economic Attack↦Banking and Finance/Business↦Economic Advantage. The first and best target from this red perspective is a state's economic health—not its armed forces.

This model fails to recognize that ends constrain means. This failure to adequately understand the primacy of ends, however, does not make Liang and Xiangsui's study of means and targets less important. There has been a sea change in the security environment. The potential for unrestricted warfare exists, and it differs in scope and kind from the Gulf War model of American materiel, intelligence and technical superiority. The differences can be attributed to many factors, especially technology, but also to a change in system structure, the emergence of different actors with nontraditional motivations and emerging "blue" vulnerabilities. This concept of unrestricted warfare helps in the analysis of how this particular red perspective views the threats, means, targets and ends of future war.

The five most frequently cited threat actors in these Chinese strategists' vision of unrestricted warfare were, in order: autonomous terrorist organizations, information warfare teams, states, hackers and state-sponsored terrorist organizations.[23] An autonomous terrorist organization is defined as a group that is political in aims and motives; is violent or threatens violence; conducts operations designed to have far-reaching psychological effects beyond the immediate victim or target; is organized with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia); and is a subnational group or nonstate entity.[24] The information warfare team is defined as a group formed by a state or nonstate actor to conduct information operations as a primary responsibility. The team does not have to be permanent and may be an ad hoc group to accomplish a specific mission. State-sponsored terrorist organizations are groups with the characteristics of an autonomous terrorist organization but that receive additional logistic, training, intelligence or other support from a state and conduct attacks in accordance with some operational guidance from that state.

The five most common means mined from this red perspective were cyberstrikes, information operations, economic attacks, bombing and direct action. A cyberstrike is defined as a concerted computer network attack (CNA) from, through and against systems to deny, damage, disrupt, alter or destroy the ability of the targeted system to function as intended. The result is system-wide in effect, and typically a cyberstrike will target a critical infrastructure system. Information operations "involve actions taken to affect adversary information and information systems while defending one's own information and information systems. Information operations target information or information systems in order to affect information-based processes, whether human or automated."[25]

This text-mining procedure applies the US military's doctrinal information operations definition, minus the CNA component. The prevalence of cyberstrike throughout this red perspective, distinct from other information operations such as deception, requires tracking with a separate code. The code "economic attack" was added to the means taxonomy in Figure 1 as a result of its emphasis in the source document and is defined as attacking an opponent's economic interests through trade sanctions, freezing financial and other assets, currency destabilization or hostile trade practices such as commodity dumping.[26] "Bombing" means using an unconventional bomb and does not include bombing by air forces during an overt conflict. "Direct action" is a physical attack directly against a target, whether by a uniformed, armed force or guerrilla or terrorist forces.

One would like to know what potential opponents are thinking. Some intelligence tools like satellite reconnaissance have limited utility to determine intent, when capabilities such as cutting-edge WMD development programs are the target. Likewise, electronic eavesdropping may be deaf to encrypted communications over fiber-optic networks.

In emphasizing both nonphysical and physical means, this red perspective advocates an eclectic mix in unrestricted warfare. It is probable, based on this red perspective, that conflict would not be strictly confined to a physical military confrontation between uniformed forces. Rather, analysis reveals that complementary physical and nonphysical means will be employed immediately in a conflict.

The target sets mentioned by the Chinese strategists are relatively few. The most emphasized target from this red perspective is the US banking and finance system. Second is business, the major corporations that make up the core economy of a state for either substantive or symbolic effect. An example of this code's use is the targeting of US corporations by foreign intelligence services to provide their nation's corporations a competitive advantage. Third is the US population, and fourth is a conglomeration of systems that collectively describe US critical infrastructure as defined by *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*.[27] The banking and finance system is a component of critical infrastructure, but like the emphasis on cyberstrikes as a subcomponent of information operations, the heavy emphasis on targeting the US banking and finance system by this particular red perspective makes it necessary to track it with a unique code.

The targets chosen indicate a strategy that bypasses American military strength while directly attacking critical infrastructure and population. Coupled with asymmetric and anonymous methods, this approach could inflict great damage. Without an identifiable enemy, retaliation is difficult. The ability to threaten America's homeland with significant new concept weapons potentially arms an opponent with a strategic deterrent. The efficacy of US saber rattling and heavy-handed diplomacy decreases when the opponent can inflict harm on American infrastructure and population.

The five most cited ends within this red perspective are national security advantage, economic advantage, financial gain, political influence, and political change. National security advantage is defined as the goal of obtaining an advantage over an opponent to further security of a state or nonstate actor. The advantage can be tangible or intangible in any instrument of power. Economic advantage is defined as the goal of obtaining a competitive advantage in the economic realm by a state or nonstate actor. Financial gain is defined as the goal of obtaining wealth in currency, commodities or other vehicles of wealth transfer. The code political influence is defined as the goal of obtaining influence in a political system for furthering interests of the actor pursuing the strategy. Political change is defined as the goal of causing a significant change in another actor's political structure through a deliberate strategy of attack using any instrument of power.

The ends emphasized in this red perspective overlap all four instruments of power: military (national security advantage), economic (economic advantage/financial gain), diplomatic/political (political change) and informational (political influence). From this red perspective, any end that increases power is worth pursuing. Regardless of the threat portrayed, means employed or target set chosen, this red perspective describes a rational actor seeking to maximize power. This trait makes calculation of this actor's purpose in executing strategies relatively easy, if its operations are discovered. Figure 3 clarifies relationship chains among Threats↦ Means↦ Targets↦ Ends.

After mining text, data can be manipulated to show relationships. For instance, an analyst interested in seeing the relationship of different means cited to obtain a given end could sift the data for all occurrences of the specific end's code tied to any means' codes. This pairing would give the analyst insight into the red perspective's thoughts regarding preferred means to obtain a certain end. The permutations and combinations that can be analyzed for insight are almost limitless, but a caution is necessary. The ability to see patterns and linkages once removed from the original source is invaluable for understanding the actor, the original source itself and for gleaning relevant security policy insights. However, further manipulation of extracted data may have a breaking point for pragmatic intelligence analysis. Looking at relationships twice or more removed from the original source, or reprocessing already refined data, may have diminishing returns in qualitative analysis. At some point, additional manipulation of data may yield valid statistics about what was said but does not enhance understanding of what was meant. Where this point lies depends on the source and the research questions explored by the analyst. Qualitative analysis is a powerful tool, but it requires common sense and judgment to yield intelligence.

We want to know who the threats are, the means they intend to use, their targets and the ends they are pursuing. This is fairly easy when dealing with an opposing state, overt conflict and announced war aims. A greater challenge is understanding emerging threats in the current security environment.

The most common chain in the form of Threat↦ Means↦ Target↦ End cited by the Chinese strategists reveals a pattern of State↦ Economic Attack↦ Banking and Finance/Business↦ Economic Advantage. This chain suggests that this red perspective considers economic issues important enough to spark some level of covert conflict to change relative economic power relationships between actors. The banking and finance and business sectors were viewed as key targets. From an American perspective, an effective attack on the US financial infrastructure would clearly be a significant event. But this red perspective's emphasis on business as a key target may differ from an American perspective, in that business is not a direct agent of the state.[28] Interpretation of this chain, as with all chains mined from qualitative analysis, should not be inflexible. Within the text passages forming the foundation of this chain are allusions to economic espionage, assistance of private corporations by state intelligence agencies, economic strength as a lever for regional political control, economic intimidation and other related thoughts. The point is that in pursuing unrestricted warfare, the first and best target from this red perspective is a state's economic health—not its armed forces.

A very close second in terms of emphasis is the chain Information Warfare Team/State↦ Cyberstrikes↦ Critical Infrastructure↦ National Security Advantage. This chain heightens the intensity of conflict by engaging a broad target set that has physical implications resulting from damage. It also has the end of gaining a national security advantage by improving principally military and diplomatic measures of relative power relationships. Targeting critical infrastructure fits a strategy of avoiding strength and attacking weakness.

This red perspective is state-centric in its viewpoints, not surprising given the source of data. However, the state in the chains above initiates conflict as a covert actor portraying another actor, portending a possible future of targeted states engaged in shadow warfare against unknown actors. Neither of the above chains dictates that the state must remain covert, but analysis of both chains suggests the initial phase of conflict will be a surprise attack by a covert actor.

Additional chains and other products and metrics can be extracted from the data, but these examples show how qualitative analysis can be useful. The ability, automated but human-driven, to mine many sources provides analysts with value-added material and increases insight. One interpretation of this specific red perspective could be that in a war with China, America's private and public economic interests will be attacked abroad and at home and, perhaps simultaneously, computer network attacks will be launched against critical infrastructures. This is a different scenario than military forces facing off around the Taiwan Strait. Brinkmanship with an opponent actually operating from this perspective may involve greater risk of unintended escalation than the six days of the Cuban Missile Crisis in October 1962.

Text mining is an important tool for understanding blue and red perspectives in a fundamentally changed security environment. Such understanding

Figure 3: **Emphasized Threats, Means, Targets and Ends**

Threats	Means	Targets	Ends
Autonomous Terrorist Organization	Cyberstrike	Banking and Finance	Security Advantage
Information Warfare Team	Information Operations	Business	Economic Advantage
State	Economic Attacks	Population	Financial Gain
Hackers	Bombing	Critical Infrastructure	Political Influence
State Sponsored Terrorism	Direct Action	Critical Infrastructure	Political Change

is a prerequisite for crafting effective national security policies. During conflict, qualitative analysis can prove a valuable source of information, enhancing the offensive and defensive use of force. The importance of text and data mining increases as other strategic intelligence tools decrease in efficacy, due to target characteristics.

Any actor articulating a perspective, whether a state or a terrorist organization, can be modeled using qualitative analysis. Source data can be a manifesto (such as the Unabomber's) or a web page. Friendly, neutral or hostile (blue, gray or red) perspectives can be modeled with results that enhance security. Qualitative analysis can also serve as a mirror that shows how others perceive oneself.

Unrestricted Warfare was used as an illustrative example in this article but is not an official statement of Chinese doctrine for future war; it is a thoughtful statement by two Chinese strategists. The framework of the document reflects the authors' background as military officers and explores the nature of a potential war between China and the United States. Mining many such documents yields insights. Threat kingdom actors should be priorities for qualitative analysis techniques.

Without a clear, reliable articulation of an actor's future policy the next best sources of information are the thoughts of that actor's security elite, available from many open sources, such as speeches, articles, books, interviews and policy papers. Qualitative analysis is not limited to text, but could include sources from video to intercepted cellular phone transmissions. Any single information source is of unknown utility for knowing another actor's intent. Text and data mining can sift all available information sources, real-time and archived, extract key information from noise and clarify patterns and linkages not visible to human analytical techniques.

Determining intent is difficult, but it is not mind reading. In a security environment where significant capabilities proliferate out of control, assuming another actor's capability is prudent. Determining intent therefore remains key in identifying threats to American interests. ***MR***

NOTES

[1] J. David Singer, "Threat-Perception and the Armament-Tension Dilemma," *Journal of Conflict Resolution*, Vol. II, (March 1958), 94.

[2] George F. Kennan, "'X,' The Sources of Soviet Conduct," *Foreign Affairs*, XXV (July 1947), 566-82.

[3] John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy* (Oxford: Oxford University Press, 1982), 89.

[4] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, trans. Foreign Broadcast Information Service (Beijing, China: PLA Literature and Arts Publishing House, February 1999), 10.

[5] Colin Elman and Miriam Fendius Elman, "Lakatos and Neorealism: A Reply to Vasquez," *The American Political Science Review*, Vol. 91, (December 1997), 923-926.

[6] These broad tenets generally describe what is known as a Realist perspective of the international system. There are other perspectives. Those interested in a primer can see Phil Williams, Donald M. Goldstein and Jay M. Shafritz, eds., *Classic Readings of International Relations*, 2d Edition (New York: Harcourt Brace College Publishers, 1999).

[7] For documentation of US vulnerability to strikes against population and critical infrastructure see George J. Tenet, "Statement of the Director of Central Intelligence," before the Senate Armed Services Committee Hearing on Current and Projected National Security Threats, 2 February 1999, Washington, DC; Lieutenant General Kenneth Minihan, NSA Director, statement before the Senate Governmental Affairs Committee hearing on "Vulnerabilities of the National Information Infrastructure," Washington, DC, 24 June 1998; and President William J. Clinton, "Remarks by the President on Keeping America Secure for the 21st Century," a speech delivered to the National Academy of Sciences (Washington, DC: Office of the Press Secretary, 22 January 1999).

[8] Liang and Xiangsui, 21-22.

[9] Ibid., 21.

[10] *Merriam-Webster's Collegiate Dictionary*, 10th ed. (Springfield, MA: Merriam-Webster, 1998), 643.

[11] Liang and Xiangsui, 107.

[12] Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith (Oxford: Oxford University Press, 1971), 101.

[13] Liang and Xiangsui, 6.

[14] Ibid., 19-22.

[15] Ibid.

[16] Ibid., 21.

[17] Ibid. Note: there are many similarities between CBNR agent use, cyberstrikes, and the Cold War model of nuclear weapons use. One similarity is that targeting civilian populations with CBNR agents or critical infrastructure with cyberstrikes approximates the Cold War strategic deterrent capability of targeting cities with Inter Continental Ballistic Missiles. A dissimilarity is that retaliation is impossible against an asymmetric, anonymous actor.

[18] Ibid., 22.

[19] Ibid., 29-30.

[20] Even genetic research aimed at creating helpful treatments and involving strict medical research protocols in a scientifically advanced nation can go wrong, as the death of 18-year old Jesse Gelsinger proves. Gelsinger was being treated at the University of Pennsylvania's Institute for Human Gene Therapy when the gene therapy designed to correct his health disorder killed him. "Gene weapons," with their explicit design to inflict harm on a large scale, could be catastrophic if released. As an example of the potential for and consequences of loss of control of so-called "new concept weapons," consider the accidental release of an anthrax bioweapon, engineered to incorporate at least four distinct strains of *Bacillus anthracis*, at a secret Soviet biological weapons facility near Sverdlovsk, Union of Soviet Socialists Republic, in April 1979. The precise extent of exposure is unknown, but involved hundreds, perhaps thousands, of deaths. For further information on Gelsinger and the University of Pennsylvania's gene treatment, see Jeffrey P. Kahn, *Gene Therapy on Trial* (Minneapolis, MN: University of Minnesota Center for Bioethics, 8 February 2000), document at <http://www.cnn.com/2000/HEALTH/02/07/ethics.matters/ethics.matters.html>. For further information on the Sverdlovsk incident, see Paul J. Jackson, et al. "PCR Analysis of Tissue Samples from the 1979 Sverdlovsk Anthrax Victims: The Presence of Multiple *Bacillus anthracis* Strains in Different Victims," *Proceedings of the National Academy of Sciences*, Vol. 95, (February 1998), 1224-1229, document at <http://www.pnas.org/cgi/reprint/95/3/1224>.

[21] Liang and Xiangsui, 6.

[22] Ibid., 11.

[23] Content analysis was conducted using accepted standards for qualitative analysis methodology in the political science field. Interested individuals can consult Udo Kelle, ed., *Computer-Aided Qualitative Data Analysis: Theory, Methods, and Practice* (Thousand Oaks, CA: Sage Publications, 1995) for an overview. Software packages used included both open-source code and commercial packages.

[24] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 43.

[25] Joint Publication 3-13, *Joint Doctrine for Information Operations* (Washington, DC: Joint Chiefs of Staff, 9 October 1998), vii.

[26] A second means was added as well—Genetic Agent, a pathogen designed to alter genetic material in crops, livestock or humans.

[27] The US critical infrastructure is comprised of key sectors that are essential to the minimum operations of the economy and the government, directly impacting on the US population. These infrastructures are information and communications, continuity of government services, banking and finance, water supply, electrical power, oil and gas production and storage, transportation, emergency services, and public health services. See *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (Washington, DC: Executive Office of the President, 22 May 1998).

[28] These strategists view systems as highly centralized and "brittle." They are partly correct regarding some systems. However, infrastructures also are robust, redundant, resilient and recuperable. Systems analysis of targeted infrastructures would reveal unique traits and degrees of vulnerability.

Lieutenant Colonel Bill Flynt is a foreign area officer with the Foreign Military Studies Office, Fort Leavenworth, Kansas. He received a B.A. from The Ohio State University, an M.P.A. from Cornell University, an M.M.A.S. from the School of Advanced Military Studies and is completing a Ph.D. focusing on National Security Policy at the University of Kansas. He is a graduate of the US Army Command and General Staff College. He has commanded in combat and served in a variety of staff positions, including chief, Plans and Exercise Branch, 101st Airborne Division, Fort Campbell, Kentucky; S3, 3d Brigade, 101st Airborne Division; and S3, 2d Battalion, 187th Infantry Regiment, 101st Airborne Division. His article, "Threat Convergence," appeared in the September-October 1999 issue of Military Review.