REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
14-02-2005	FINAL	

4. TITLE AND SUBTITLE

Defeating a Transformed U.S. Military

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Maj G. Todd Puntney, USMC

Paper Advisor (if Any): N/A

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

NCW, as a theory of war, relies on the premise that ubiquitously networked forces and capabilities will outperform forces that are not. Put another way, all things being equal, the side with the ability to network will generally win. Fundamentally, then, the key enabler of NCW is represented by the functioning of the network that connects sensors, shooters, and decision makers in a system exploiting the synergy of its dispersed parts.

While the ubiquity and health of the network is therefore paramount, weapons designed to attack the electronic components of that network can, in an instant, vaporize U.S. technological and operational superiority and render future, NCW-based combatant commanders and military forces impotent.

This paper explores the relationships between NCW, systems and chaos theories, Col. John R. Boyd's decision making model, and their impact on a potential operational center of gravity and its subsequent vulnerabilities; identification of likely threats posed by potential adversaries to hold our networked forces at risk; and recommended solutions to defend against those threats.

15. SUBJECT TERMS

Network-Centric Warfare, Transformation, Systems, Chaos, Critical Vulnerabilities, Threats, Electromagnetic Pulse

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		26	19b. TELEPHONE NUMBER *(area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Defeating a Transformed U.S. Military

By

G. Todd Puntney
Major, U.S. Marine Corps

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

14 February 2005

ABSTRACT

Network-centric warfare (NCW), as a theory of war, relies on the premise that ubiquitously networked forces and capabilities will outperform forces that are not. Put another way, all things being equal, the side with the ability to network will generally win. Fundamentally, then, the key enabler of NCW is represented by the functioning of the network that connects sensors, shooters, and decision makers in a system exploiting the synergy of its dispersed parts.

While the ubiquity and health of the network is therefore paramount, weapons designed to attack the electronic components of that network can, in an instant, vaporize U.S. technological and operational superiority and render future, NCW-based combatant commanders and military forces impotent.

This paper explores the relationships between NCW, systems and chaos theories, Col. John R. Boyd's decision making model, and their impact on a potential operational center of gravity and its subsequent vulnerabilities; identification of likely threats posed by potential adversaries to hold our networked forces at risk; and recommended solutions to defend against those threats.

> *For want of a Nail the Shoe was lost; for want of a Shoe the Horse was lost; and for want of a Horse the Rider was lost; being overtaken and slain by the Enemy, all for want of Care about a Horse-shoe Nail.*[1]
> **BENJAMIN FRANKLIN**

Benjamin Franklin, more than two centuries ago, described the law of unintended consequences: in complex and dynamic environments, the smallest action, regardless of its sincerity or rationality, has the potential to breed unanticipated and obscure side-effects and expose, through hindsight, what are otherwise hidden vulnerabilities.

In its current form, the implementation of network-centric warfare is to the U.S. military what the nail is to the rider, and the distance between the two exposes the potential for not ephemeral but conspicuous, menacing defects. "The working hypothesis of network-centric warfare (NCW) as an emerging theory of war, simply stated, is that the behavior of forces…when in the networked condition, will outperform forces that are not."[2] It follows, then, that when the combat effectiveness qualities between competing military forces are equal, the side with the ability to network will generally win. Therein smolders the weakness: what happens when a joint task force, trained and organized to function in a networked environment, suddenly finds itself disconnected?

While the ubiquity and health of the network is therefore paramount, weapons designed to attack the electronic components of that network can, in an instant, vaporize U.S. technological and operational superiority and render future, NCW-based combatant commanders and military forces impotent.

Determining and obviating the vulnerabilities of such a force requires an analysis of NCW theory and its inferred relationships with systems theory and Col. John R. Boyd's decision making model, an assessment of a future NCW-enabled operational center of gravity and its potential critical vulnerabilities, the implications of chaos theory on methods

to exploit those vulnerabilities, and the likely threats posed by adversaries to hold our networked forces at risk.

COMPARISONS OF THE THEORIES BEHIND THE THEORY OF NCW

At its heart, network-centric warfare is conceptually bounded by systems theory, the study of the relationships between the parts of a system and the fundamentally different properties that emerge when a system is evaluated as a whole rather than when its individual components are viewed in isolation.[3] From an NCW perspective, the potential for an exponential increase in combat effectiveness is derived from the collective functioning of a tremendously connected grouping of forces. Indeed, "this linking of people, platforms, weapons, sensors, and decision aids into a single network creates a whole that is clearly greater than the sum of its parts."[4] Unlike wars of the past—qualified by the time-consuming massing of forces with relatively few interconnections and a limited view of the battlespace—NCW, comparatively speaking, promises to dispense with such Industrial Age sentimentalities. Orders of magnitude in increased effectiveness can be achieved with a focus less on individual platforms or weapons systems and more on the synergism their effective linking brings. The immediate and opportunistic application of precision firepower yields smaller forces, dispersed throughout the battlespace but sharing a common awareness, relying not on heavily armored formations and a logistically burdensome infrastructure but instead on mobility and tempo to wield greater combat power potential and an ability to better adapt to and survive the complexities spanning the spectrum of conflict.[5]

With systems theory, the ability of a system and the relationships between its parts to cope with interaction in a dynamic environment determines whether or not it can thrive in a state of complexity. If it cannot, it veers toward equilibrium ("a state in which the system is incapable of any productive activity") or toward chaos ("a state in which there is a great deal

of activity but no purpose or direction").[6] NCW's focus on the ubiquitous networking of forces smoothes the connections between system parts and amplifies our ability to thrive in the dynamic, tumultuous circumstances of combat.

Elementally, network-centric warfare is "about human behavior within a networked environment" and the changes that occur to organizational structures and methods of performance when connected together.[7] This relatively intangible behavior, this ability "to network," is regarded as distinct from what ordinarily is viewed as NCW, or the technology represented by "the network."[8] The distinction is important in that it defines how we are to characterize NCW, but it also begs the question: if NCW is, primarily, about human behavior, what aspects of that behavior does it seek to address? The decision making model of Boyd's observe-orient-decide-act (OODA) loop provides an interesting analysis.

The OODA loop describes a continuous and repeating cycle of interactions within a system and with its environment. Information, in terms of how it is interpreted by humans and what they do with it, represents a critical factor in the process. Table 1 compares key similarities between the OODA process and the four tenets of NCW.

Table 1.[9]

OODA LOOP	TENETS OF NCW
OBSERVE a situation.	*"A robustly networked force improves information sharing"*—If individuals, organizations, or systems are physically or logically connected to one another, then it follows that they can exchange information and thereby share observations.
ORIENT to that observation by analyzing and synthesizing its factors and developing a meaningful interpretation of that observation.	*"Information sharing enhances the quality of information and shared situational awareness"*—The more entities that can sense events, that can make observations and shape those within the framework of a common picture or understanding, can better interpret the reality of the battlespace.[10]
DECIDE on a course of action based on that interpretation and then **ACT** on that decision. Decisions and actions are shaped by *schwerpunkt*—the "unifying medium that provides a directed way to tie initiative of many subordinate actions with superior intent as a basis to diminish friction and compress time."[11]	*"Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command"*—Individuals and organizations, based on that common orientation and shaped by a unifying principle—commander's intent—can adapt, respond, and operate in a flexible, near autonomous fashion at the lowest levels.
RECYCLE, rapidly, through the steps.	*"These, in turn, dramatically increase mission effectiveness"*—Self-synchronization, as a by-product of reduced internal friction and external fog, thus enhances the speed of the cycle and reinforces the focus on the enemy.

Combat represents a clash between OODA loops and the competitive struggle to cycle faster through it than the enemy in order to present him with an array of situations for which he cannot cope, to get inside his loop "to enmesh [an] adversary in a world of uncertainty, doubt, mistrust, confusion, disorder, fear, panic, chaos…and/or fold [an] adversary back inside himself."[12] Creating such complexity for the enemy "causes commanders and subordinates alike to be captured by their own internal dynamics or interactions—hence they cannot adapt to rapidly changing external (or even internal) circumstances."[13]

The goal, then, is to protect friendly cohesion by internally limiting the effects of friction and unifying the parts of the system to function as a whole, so that the loop can recycle faster and efforts can be concentrated externally against the enemy. It is, foremost, about human behavior. NCW, with its power derived from a networked sum-of-the-parts system, is the application of Boyd's OODA loop to the Information Age.

AN OPERATIONAL CENTER OF GRAVITY

Applying the Joint definition as "sources of power from which a military force derives its freedom of action, physical strength, or will to fight,"[14] our center of gravity points to the intersection of the four tenets of NCW, for they "constitute a hypothesis regarding NCW as a *source of power*" (emphasis added).[15] To go further, if NCW can indeed exert such tremendous influence on our warfighting strength, then its critical capability, that which allows it to function as a center of gravity, is the ability of individuals and organizations "to network" and collectively operate in unison toward a common goal. While NCW's focus is on human behavior, the circularity of the argument suggests that such behavior can only be enabled by technology. The critical requirement, therefore, of the

ability "to network" is the value derived from and the ubiquitous functioning of "the network."

Boyd's analysis of the "Strategic Game"—"a game in which we must be able to diminish [an] adversary's ability to communicate or interact with his environment while sustaining or improving ours"[16]—underscores the criticality of "the network." Based on several esoteric scientific and philosophical theories, he asserts that a system cannot determine its own character or nature in and of itself and that

> [a]ttempts to do so lead to confusion and disorder—mental as well as physical. Point: We need an external environment, or outside world, to define ourselves and maintain organic integrity, otherwise we experience dissolution/disintegration—i.e., we come unglued….If we don't communicate with [the] outside world—to gain information for knowledge and understanding as well as matter and energy for sustenance—we die out to become a non-discerning and uninteresting part of the that world.[17]

Therefore, once the ability of a system to communicate within itself and with the outside world is severed, its OODA loop stretches and its cohesion necessarily begins to falter. The critical vulnerabilities of our center of gravity, then, lurk in the depths between "to network" and "the network" and the interaction between the two: a resourceful enemy may find that attacking the technology to influence the human behavior is the surest path to our defeat.

CHAOS THEORY

Chaos theory provides insights into system disruption and the likelihood that, based on the dynamic interaction of a system and the rules that define how its components change, a system will behave unpredictably.[18] Chaos—erratic behavior based on irregular, even simple, dynamics—threatens the stability of a system.[19] Systems that are susceptible to chaos are particularly sensitive to initial conditions, meaning that small changes to a system can result in unpredictable consequences; they are, therefore, extremely vulnerable to "external perturbations, or 'kicks.'"[20] Feedback mechanisms, furthermore, amplify the propensity for

chaos, in that "Chaos appears when the system *has insufficient time to relax and recover* before the next 'event' occurs."[21] Excessive, delayed, or incorrect feedback—no matter how infinitesimal the size—creates the potential to shove an otherwise orderly system into havoc.

Introducing chaos into a complex system can therefore lead to its unraveling. Within the context of NCW and the critical requirement of "the network," communications systems display a marked propensity for chaos: "The high volume and speed of communication through computer networks includes the best ingredients of a recipe for Chaos: modular processes undergoing endless iteration; frequent feedback in communications 'handshaking'; and frequencies (on many scales) faster than the time it takes most systems to recover between 'events.'"[22] Chaos in the network leads to chaos in the OODA loop, which, as a process that continually changes and requires feedback, itself is susceptible to chaos.[23] Since warfare is "path-dependent" and sensitive to initial conditions,[24] chaos can become a determinant of victory or defeat.

ATTACKING CRITICAL VULNERABILITIES

How best, then, to insert chaos in our network? How best to disrupt or deny the network to shape human interpretations and actions, to drive us toward equilibrium (no activity) or chaos (lots of activity but with no purpose)?

Computer network attacks, viruses, worms, Trojan horses – all are easily recognizable terms in today's lexicon of network threats and represent a component of Information Age warfare. As well, skillful operational deception to shape our perceptions of the battlespace may disrupt our OODA loop and create that momentary pause in decision making that alters our course of action. In both instances, however, we have recognized such vulnerabilities and have sought to ameliorate them: whether it's fielding sturdy and defended hardware and software systems, utilizing networks to which the enemy does not ordinarily have access,

applying responsive command and control techniques (such as mission-type orders and commander's intent), or cultivating in our commanders through pervasive education the intellectual rigor necessary to cope with adversity in battle, we have developed compensating mechanisms to help stabilize our system before or when it veers toward the edge.

But, assuming that "military competition is continuous and no military is as thoroughly studied as our own,"[25] potential adversaries most likely will look for vulnerabilities beyond those that we have attempted to address and will explore more permanent and debilitating means to offset our advantages. If our network defenses are too rugged or the intuitive minds of our commanders too wily, the most promising application of Information Age warfare to attack our network may depend less on deception or spurious 1's and 0's and more on our susceptibility to warheads that pack an electromagnetic wallop.

THE ONCE AND FUTURE THREAT

Oddly, the threat tomorrow—the most direct challenge to our revolutionary way of warfare—is one we saw yesterday. High-altitude Soviet and U.S. nuclear tests demonstrated a phenomenon remarkable not only in its potential for widespread impact but also in its proclivity for electronic evisceration. During a particularly illuminating test in 1962, an electromagnetic pulse, generated by radiation interacting with the atmosphere, created a radio frequency wave of such intensity that, 1,400 km away in Hawaii, street-lights popped and circuit breakers tripped.[26] The repercussions of that event resonate into our future.

An electromagnetic pulse (EMP) is an infinitesimally short but extremely intense gush of electromagnetic energy that can produce thousands, even millions, of transient volts.[27] Once in the atmosphere, that pulse radiates outward until it dissipates; in the intervening period, it's attracted to and channeled by electrical conductors. For electronic equipment operating within such an environment, the consequences can be alarming.

Energy generated by an EMP penetrates or is conducted to equipment through the "front door," where electromagnetic energy is coupled through strong electrical conductors such as antennas, or the "back door," where that energy is coupled through unintentional antennas, such as telephone wires, coaxial cables, power lines, even water pipes.[28] In both instances, the energy is propagated through the conductor and into the electronic equipment itself. Since electromagnetic energy penetrates most structures and environments, equipment inside—unless it's thoroughly protected against such effects—remains permanently susceptible; in cases of protected facilities, the smallest openings (from doorways to windows to line conduits) provide pathways for energy propagation.[29]

Solid-state semiconductors and microelectronics—all components of Information Age systems—are extremely sensitive to electrical charges and are designed to operate within very specific tolerances. Once an electric charge enters an electrical component and surpasses the threshold of the component's ability to dissipate that charge, the proper functioning of the equipment is threatened. With a "hard kill," electromagnetic energy, amply applied, produces thermal damage to components; with a "soft kill," components, even with an extremely small amount of spurious energy, continue to operate but in an intermittent and degraded fashion.[30]

From a strategic perspective, a well-placed nuclear detonation high above the central U.S. has the potential to gut all manner of national infrastructure, including power generation and distribution, banking, telecommunications, transportation, and agriculture. The Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (EMP Commission) studied that eventuality and, hauntingly, declared that it "is one of a

small number of threats that has the potential to hold our society seriously at risk and might result in the defeat of our military forces."[31]

Militarily, 1962 exposed a tremendous vulnerability. Recognizing the potential threat to strategic nuclear forces, in particular, the U.S. developed a thorough program designed to protect not only the weapons and their delivery platforms but also the command and control structure necessary for their launch.[32] The viability of a U.S. nuclear response was therefore assured.

While terrifying to imagine in both its simplicity and scope, an EMP generated by a high-altitude nuclear detonation may not be the most likely threat posed to a network-centric force. Given the likelihood that use of a nuclear weapon would induce a debilitating U.S. response as well as generate significant geopolitical fallout, such an attack, particularly by a peer competitor, is relatively self-deterring.[33] Regrettably, technological advances have demonstrated that an EMP can be generated without the employment of strategic nuclear weapons, and so its effects can materialize at the operational level of war.

Flux compression generators, which convert the mechanical energy of an explosive into a magnetic field, to vircators, which create exceptionally strong high power microwave pulses, are technically feasible and encompass an array of mature technologies.[34] Indeed, U.S. and Soviet (and then Russian) experimentation and development of such weapons began more than 40 years ago.[35] Such non-nuclear electromagnetic warheads can be used in bombs, missiles, or artillery rounds, and, since they can be made directional, afford an enemy the advantage of employment without the potential for widespread electronic fratricide in an area of operations. Given the inclination, "any nation with even a 1940s technology base, once in

possession of engineering drawings and specifications for such weapons, could manufacture them," with dollar costs in the low thousands.[36]

The vulnerabilities to combatant commanders posed by non-nuclear EMP devices are an extension of our illusory concern of the EMP threat. With the end of the Cold War, as the specter of nuclear confrontation faded with the demise of the Soviet Union, the focus on defending against an EMP attack left the consciousness of military planners and "gave rise to the perception that an erosion of EMP survivability of military forces was an acceptable risk."[37] As well, little attention during the height of the Cold War—and less since—was paid to the EMP protection of less-than-strategic capabilities, while, simultaneously, shrinking military budgets and a craving for affordable and advanced information technology equipment developed by the private sector resulted in an addiction to commercial-off-the-shelf (COTS) products. The EMP Commission illuminates our weaknesses: "Our increasing dependence on advanced electronics systems results in the potential for an increased EMP vulnerability of our technologically advanced forces, and if unaddressed makes EMP employment by an adversary an attractive asymmetric option."[38] Since it's difficult to imagine that future enemies will so readily defy strategic and operational logic, as did Saddam Hussein, and accept U.S. technological superiority on the field of battle, the employment of non-nuclear EMP weaponry to counter an NCW-enabled force would appear to be agreeably lucrative.[39]

What, in particular, is vulnerable? Aircraft, ships, tanks, fire control and fire direction systems, precision weapons, air defense and navigation systems, sensors, radars, electronic countermeasures, generators, water purification units, trucks, bulldozers, medical equipment, tactical and commercial telephones, switchboards, satellite and terrestrial radio systems,

ground segment stations of satellite networks, servers, routers, computers, printers, plasma displays, LCD projectors—a depth and breadth of systems packed with electronic components and employed by operational commanders. Unless a system or component has been designed with EMP in mind, which, in the case of most COTS equipment, is hasn't, then the system is threatened. Even if a system or component is afforded some manner of protection, the slightest gap in those defenses—an open compartment, a cracked case, a drilled hole—creates a conduit of vulnerability.

DEFEATING A TRANSFORMED U.S. MILITARY

If our critical vulnerabilities stem from the functioning of "the network" and its influence on the ability "to network," if an inability to communicate within the system or with the environment detrimentally focuses our efforts internally, if the communications systems that encompass the network and the OODA loop that reflects human behavior are sensitive to chaos, if meaningful chaos can erupt from simple interactions that vibrate disproportionately throughout the system as a whole, and if an enemy seeks to bypass our strong-points and attack us asymmetrically where we are weakest to push us into equilibrium or chaos, then it follows that EMP weaponry—on multiple levels—can deliver the shock that shatters our cohesion. Few weapons, if any others, provide such a technological antidote to NCW.

Practicably, an attack against a command and control node, based on the intersection of both systems and chaos theories, may result in cascading effects that ripple throughout the system. While data networks, for instance, can sense traffic conditions and adjust the routes through which information flows, in the event a smaller tributary—or series of them—is eliminated, automatic rerouting across the system may induce stresses that increase latency, reduce throughput, or cause network failure. As well, equipment not taken permanently off-

line by an EMP may suffer enough only to cause intermittent operation, thus reducing its effectiveness to sense, shoot, or communicate, with subsequent cascading effects on the decision making cycle.

Indeed, lack of the network or communications connectivity would necessarily isolate a commander, thus reducing the decision making process to an academic exercise.

> Stopping the outward flow of information produces paralysis, as commands cannot reach the elements which are to execute them. Stopping the inward flow of information isolates the decisionmaking element from reality, and thus severely inhibits its capacity to make rational decisions which are sensitive to the currency of the information at hand.[40]

For NCW-enabled combatant commanders and forces, such an occurrence could be vexing. So, imagine a particularly defining, worst-case moment in the future:

An operational commander, linked in a “system of systems” to his self-synchronizing forces and empowered by perceptual sharpness forged from shared awareness, develops an intuition and comprehension of the battlespace. His staff, enmeshed in an operations center filled with an abundance of displays and command and control systems and radios, translates and distributes his mission and intent to ensure the commander’s mind and his forces harmonize together in unified effort to accomplish the mission. While the fog of war remains, the reality of the battlespace, comparatively, is better discerned than it was a decade ago and the ability to function in the hazy, complex environment of combat is relatively simplified; NCW has greased the OODA loop. Indeed, based on the doctrine and training and technology of the time, there is no other ordinary way for the commander or his staff to function.

Suddenly, EMP-equipped cruise missiles, launched by an astute and cunning and studied enemy, detonate in the general vicinity of a number of friendly command posts and

ships at sea, which had been identified and targeted based on their electronic emissions. The initial attacks introduce chaos into the system, "the network," and set in motion a chain of events that weaken it; seconds later, air-dropped EMP bombs push the system over the edge.

Other than the distant reports of surprisingly few explosions, the operational commander knows only that, both literally and figuratively, it has become dark. While there is no physical damage to speak of, no smoldering ruins of destroyed facilities, he and his staff remain alive and conscious, only mute.

What happens next, when the enemy launches air, sea, and ground attacks, is problematic. Friction ensues as the commander tries to communicate with higher, adjacent, and subordinate forces to sense something, anything. Lacking feedback, his staff and his OODA loop become disjointed, and, lacking an ability to exert influence, he hopes that his commander's intent unifies the efforts of his forces. Farther down the chain of command, though, split apart as well from the network, organizational blindness separates units from one another and shared awareness and common action suddenly become irrelevant concepts of the past. What was once simple, what was once trained to and expected, becomes horribly complex. What was once routine, such as firing a weapon, becomes impossible. What was once a tightly knit, mutually supporting, synergistic coupling of dispersed forces now becomes a fractious, broken, lonely collection of individuals fighting individual battles.

And what was once a compelling theory of war becomes a hollow pathology of defeat.

RECOMMENDATIONS

Of course, it's unreasonable to assume that such a worst-case scenario is preordained or within the realm of "highly probable." Indeed, for an enemy to catch us so off-guard would imply a level of negligence well beyond the scope of EMP protection. Friendly air

defenses, operational security and emissions control measures, and indications and warning—not to mention our own likely ability to deliver conventionally generated EMP effects—offset forecasts of doom. But in instances when we don't fire the first shot or when we suffer from a sneak attack (which our history validates), our current susceptibility to an EMP has operational and strategic implications.

As an operational function, protection of "the network" is recognized as an essential condition for the effects of NCW to be realized.[41] When it comes to the vulnerabilities posed by EMP, however, we have lacked the prescience to holistically implement solutions. While the EMP Commission notes that the Department of Defense's acquisition process specifies certain EMP protection requirements, "adherence to [this] policy…has been spotty, and the huge challenge of organizing and fielding an EMP-durable tactical force has been a disincentive to applying the rigor and discipline needed to do so."[42]

There are, however, effective countermeasures (both equipment- and process-based) that may be employed by, and are in some cases readily available to, operational commanders and the military services:

Equipment hardening: Equipment specifically engineered with EMP in mind can be effectively hardened to withstand such electromagnetic assaults, but effort and cost considerations necessitate implementation during the design phase. As well, hardening should be applied to the system as a whole, as damage to "any single element of a complex system could inhibit the functioning of the whole system."[43] Hardening holistically, after a system has been produced, may be cost prohibitive; new "transformational" programs supporting NCW, therefore, should have hardening built-in, with cost increases in the range of one to five percent of the system cost.[44]

Shielding defense-in-depth: Electrically conductive enclosures, known as Faraday cages, isolate equipment and components from electromagnetic energy and therefore provide protective shields from an EMP. Key strategic facilities today are afforded this type of protection. In a tactical and operational environment, however, in the location most prone to experience the effects of a localized EMP attack, no protective measures exist. Commercially available Faraday cages have practical applications for workspaces, equipment, and line transmission media.[45] Solutions, then, involve use of existing Faraday cage technology in a defense-in-depth approach, with tents protecting equipment inside, add-on covers for hardware (such as computers, servers, and power supplies), and shields for non-fiber optic cable. Future development efforts should integrate camouflage netting, tents, and general-purpose shelters that possess Faraday properties.

Cables: Coaxial and twisted-pair copper cables form the backbone of most data and telephone networks in the field, but, as excellent conductors and couplers of electromagnetic energy, serve as giant antennas to collect and propagate EMP effects. Fiber-optic cable, on the other hand, is "wholly immune" to an EMP.[46] While any widespread effort to connect everything with fiber-optic cable has its own attendant difficulties (fragility of the optics, for instance), developing and employing improved fiber-optic technology might enhance its use between and within protected spaces.

Configuration management and training: Because of the strict parameters of system design necessary to defeat an EMP, any changes to a system—or lack of adherence to those parameters—potentially threaten system integrity.[47] Set rules and procedures should be established and enforced in the field so that negligent or unintentional actions do not compromise the system as a whole. Currently, while certain radio systems, switchboards, and

technical control facilities have some level of EMP protection, they are routinely operated with doors or hatches left open, thus exposing that protection to defeat. As well, it is difficult if not impossible to determine in a technical manual if a system has EMP protective characteristics or how modes of operation might affect that protection; these should be clearly and simply enumerated. Furthermore, a designated organization (the J-6, for instance) should direct, implement, and supervise the counter-EMP effort. Once the threat is deemed serious enough to warrant a serious organizational effort to defend against it, pervasive EMP awareness could inhibit the potentially catastrophic consequences its use may offer.

Node analysis: In the short-term, an analysis of critical nodes in a communications network could provide a prioritized list of key locations for which EMP protection is absolutely essential, thus shaping funding and fielding efforts accordingly. In the long-term, instituting networking topologies that prevent inordinate centralization of information flow to a few nodes and instead distribute that flow across many nodes could offset the potential widespread effects of single points-of-failure. As well, while effective communications networks rely on a principle of path and system redundancy, additional quantities of critical equipment and components, stored off-line and in protected areas, should be procured and deployed to provide immediate, on-site replacement of EMP-damaged systems. Radios based on vacuum tube technology remain unaffected by an EMP; a fail-safe vacuum tube radio net connecting key nodes, while seemingly counterintuitive in the context of modern technology, may prove beneficial in an EMP environment.

Training: Exercises, as a rule, generally do not include training in an environment with widespread communications network failure. With the centrality of networks today, and even more so when we reach the future of NCW, we should develop training standards that

test our mettle under such conditions in order to develop the tactics, techniques, and procedures necessary to survive if the organizational lights go out—commander's intent only provides so many options for an infantry battalion attempting in vain to call for close air support.

The basics: Given the tremendous advantages NCW, theoretically, will provide us, we should not, however, forget the foundational excellence upon which our current military capabilities are based. Implementing a balance between new technologies and concepts and a set of legacy, Industrial Age capabilities—whether it's a weapon system that fires mechanically, a radio that operates with vacuum tubes, or a map that's adhered to a flip-chart and not a PowerPoint slide—may limit our vulnerabilities in the future.

CONCLUSION

Certainly, there is considerable expense—both in resources and organizational energy—to any solution. Balanced with the potential threat and our manifestly apparent vulnerabilities to an EMP, however, we can afford few other courses of action. While other modes and methods of attack may threaten the stability of our system, EMP weaponry represents a potential "silver bullet" that, at least in the current state of affairs, could have the most monumental and detrimental impact. Significant effort to harden, shield, and correctly employ electronic equipment is required to protect "the network" to prevent it from becoming "the vulnerability."

NCW is predicated on the fundamental linking of sensors, shooters, and decision makers. Based on its theoretical foundations, it seeks to empower future joint forces with capabilities synergized from its parts to rapidly and violently defeat the enemy. But when chaos denies or disrupts the network, potential side-effects loom: a stretched OODA loop, a

limited variety of responses and inhibited freedom of action, disrupted harmony, loss of initiative, and a cohesive, synergistic system reduced to a disconnected clutter of parts.

"A force implementing NCW is more adaptive, ready to respond to uncertainty in the very dynamic environment of the future at all levels of warfare and across the range of military operations."[48] The converse is then true as well: A force without the ability "to network" is less adaptive, less ready to respond, and more susceptible to defeat in detail.

We've already begun the journey down the road—we've fitted the nail in the shoe. At some point in the future, we may look back at our history and regard it as an auspicious moment, or view it, wistfully, with longing.

NOTES

[1] Respectfully Quoted: A Dictionary of Quotations Requested from the Congressional Research Service (Washington, D.C.: Library of Congress, 1989; New York: Bartleby.com, 2003). <http://www.bartleby.com/73/1240.html> [20 January 2005].

[2] Office of Force Transformation, The Implementation of Network-Centric Warfare (Washington, D.C.: 2005), 15. <http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf> [15 January 2005].

[3] Francis Heylighen and Cliff Joslyn, "What is Systems Theory?" Principia Cybernetica Web, 01 November 1992. <http://pespmc1.vub.ac.be/ SYSTHEOR.html> [22 January 2005].

[4] Office of Force Transformation, i.

[5] Ibid., 8-10.

[6] James K. Greer, "Operational Art for the Objective Force," Military Review, (September-October 2002): 27. <http://www.leavenworth.army.mil/milrev/download/English/SepOct02/greer.pdf> [21 January 2005].

[7] Office of Force Transformation, i.

[8] Ibid., 3.

[9] John R. Boyd, "A Discourse on Winning and Losing," (Unpublished Thesis, located at U.S. Naval War College Library, Newport, R.I.: 1987), 29; Office of Force Transformation, 7. Additionally, the following table explores other relationships between Boyd and NCW:

BOYD CONCEPTS (Boyd, "A Discourse on Winning and Losing," 32 (reverse), 69 (reverse), 75 (reverse))	**NCW GOVERNING PRINCIPLES** (Office of Force Transformation, 8-10)
To adapt and thrive in a complex environment:	
Rapidly apply a variety of options	Self-synchronization: Subordinate initiative increases tempo and permits rapid adaptation to the situation Speed of command: Information superiority compresses decision timelines
Harmonize efforts of system parts	Shared awareness: Translate information into common understanding Self-synchronization: Near autonomous retasking based on shared awareness and commander's intent
Maintain initiative (to influence the environment) instead of passive action (environment influences you)	Alter initial conditions: Warfare is "path-dependent" and requires rapid execution
To win: Stretch out time for the enemy, limit enemy range of options, multiply opportunities to split enemy apart, shatter enemy cohesion through surprise and shock	Dispersed forces: Non-linear operations and precision effects enhances temporal advantage Demassification: Dispersed forces complicate enemy's targeting problem Speed of command: Speed locks out enemy options Fight for information superiority: Through information advantage, limit enemy information and increase enemy uncertainty

[10] Grounded in Metcalfe's Law, which states that the value of a network equals the square of the number of nodes on a network. See Charles Boyd, "Metcalfe's Law," Management Issues, 02 February 2005, <http://www.mgt.smsu.edu /mgt487/mgtissue/newstrat/metcalfe.htm> [08 February 2005].

[11] Boyd, "A Discourse on Winning and Losing," 65 (reverse).

[12] Ibid., 137.

[13] Ibid., 122 (reverse).

[14] Joint Chiefs of Staff, Joint Doctrine for Campaign Planning, Joint Publication 5-00.1 (Washington, D.C.: 25 January 2002), GL-3.

[15] Office of Force Transformation, 19.

[16] Boyd, "A Discourse on Winning and Losing," 170 (reverse).

[17] Ibid., 168.

[18] Glenn E. James, Chaos Theory: The Essentials for Military Applications, The Newport Papers, no. 10 (Newport, R.I.: U.S. Naval War College, October 1996), 3.

[19] Ibid., 41.

[20] Ibid., 30, 49.

[21] Ibid., 17.

[22] Ibid., 51.

[23] Ibid., 62.

[24] Office of Force Transformation, 10.

[25] Ibid., 68.

[26] Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (EMP Commission), Volume 1: Executive Report (Washington, D.C.: 2004), 4-5. <http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf> [10 January 2005].

[27] Carlo Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," Air & Space Power Chronicles Online Journal, 1996: 1. <http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html> [11 January 2005].

[28] Carlo Kopp, An Introduction to the Technical and Operational Aspects of the Electromagnetic Bomb, Royal Australian Air Force Air Power Studies Centre, no. 50 (Canberra, Australia: RAAF Air Power Studies Centre, November 1996), 12. <http://www.csse.monash.edu.au/%7Ecarlo/archive/MILITARY/APSC/wp50-draft.pdf> [11 January 2005].

[29] Department of the Army, Maintenance of Mechanical and Electrical Equipment at Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities: System Design Features, TM 5-692-2 (Washington, D.C.: 15 April 2001), 27-2. <http://www.usace.army.mil/inet/usace-docs/armytm/tm5-692-2/chap27VOL-2.pdf> [11 January 2005].

[30] Kopp, An Introduction to the Technical and Operational Aspects of the Electromagnetic Bomb, 1-2. Also, Centre for Critical Infrastructure Protection, "Electromagnetic Pulse," CCIP Newsletter, Vol. 3, Issue 5 (Wellington, New Zealand: June 2004): 1-2. < http://www.ccip.govt.nz/ccipnewsletter/2004/ccip_newsletter_V3I5.pdf> [11 January 2005]: Additionally, even if equipment survives the initial EMP burst, it may be less resistant to subsequent pulses. During the 15 minutes following an initial attack, residual magnetic fields in equipment build-up and then discharge; these late-time effects may push an already stressed component over the edge.

[31] EMP Commission, 1.

[32] Kopp, An Introduction to the Technical and Operational Aspects of the Electromagnetic Bomb, 3; EMP Commission, 47.

[33] Ballistic missile defense provides hope against those not deterred, such as terrorists or rogue states.

[34] Kopp, An Introduction to the Technical and Operational Aspects of the Electromagnetic Bomb, 3, 5, 9.

[35] Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," 3.

[36] Ibid., 22.

[37] EMP Commission, 47.

[38] Ibid.

[39] The People's Republic of China, in particular and as a consequence of its economic and military growth, represents a potential adversary. See People's Republic of China State Council Information Office, "China's National Defense in 2004," Government White Papers, 27 December 2004: 1,2,4,5,7. < http://www.china.org.cn /ewhite/20041227/index.htm> [20 January 2005]: Reading the recently released official government white paper is like reading the background plot of a Cold War novel. While describing the "arduous" difficulties in developing a modern military and floridly proclaiming it seeks only a "moderately prosperous" society that threatens no one—a society, indeed, "holding high the banner of peace"—it also asserts that "tendencies of hegemonism and unilateralism" shake the stability of an emerging world order. Amidst all of the euphemistic self-deprecation and banner-waving, however, it provides a stark caveat to such pacifistic behavior: in any instance when Taiwan, particularly goaded by "foreign interference," moves toward independence, "the Chinese people and armed forces will resolutely and thoroughly crush it at any cost." Recognizing the trend of the revolution in military affairs away from mechanization and toward "informationalization," the paper further characterizes the strategic focus of the Chinese military: to build an informationalized force to win an informationalized war. Also, James R. Lilley and David Shambaugh, eds., China's Military Faces the Future (Washington, D.C.: American Enterprise Institute, 1999), 69: Published articles by Chinese military leaders and think-tanks profess the ability of "magic weapons" to enable "the inferior to defeat the superior," particularly in struggles against highly electronic foes. Weapons that pack an electromagnetic punch figure high in the range of asymmetric options.

[40] Carlo Kopp, A Doctrine for the Use of Electromagnetic Pulse Bombs, Royal Australian Air Force Air Power Studies Centre Working Paper, no. 15 (revised draft) (Canberra, Australia: RAAF Air Power Studies Centre, July 1993), 7. <http://www.csse.monash.edu.au/~carlo/archive/MILITARY/APSC/wp15-draft.pdf> [11 January 2005].

[41] Office of Force Transformation, 8.

[42] EMP Commission, 48.

[43] Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," 21.

[44] George W. Ullrich, "Statement," U.S. Congress, House, Committee on National Security, Subcommittee on Military Research and Development, Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure: Hearing before the Military Research and Development Subcommittee, 105th Cong., 1st sess., 16 July 1997. <http://web.lexis-nexis.com/congcomp/ document?_m=03888fa59248169d783c6fa47c458cb5&_docnum=30&wchp=dGLbVtz-zSkSA&_md5=da0fcdd87891abe715592cb51fd15397> [11 January 2005]. Also, Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," 21: Hardening measures that defended against nuclear-generated EMP may not be suitable for conventionally generated EMP.

[45] For a sample list of commercially available products, see <http://www.faradaycages.com/>.

[46] Carlo Kopp, “Hardening Your Computer Assets,” 1997 Reports, 22 December 2004: 2. <http://www.globalsecurity.org/military/library/report/1997/harden.pdf> [11 January 2005].

[47] Department of the Army, 27-4.

[48] Office of Force Transformation, 19.

Bibliography

Boyd, Charles. “Metcalfe’s Law.” Management Issues. 02 February 2005. <http://www.mgt.smsu.edu /mgt487/mgtissue/newstrat/metcalfe.htm> [08 February 2005].

Boyd, John R. “A Discourse on Winning and Losing.” Unpublished Thesis, located at U.S. Naval War College Library. Newport, R.I.: 1987.

Centre for Critical Infrastructure Protection. “Electromagnetic Pulse.” CCIP Newsletter, Vol. 3, Issue 5 (June 2004): 1-2. <http://www.ccip.govt.nz/ccipnewsletter/2004/ ccip_newsletter_V3I5.pdf> [11 January 2005].

Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (EMP Commission). Volume 1: Executive Report. Washington, D.C.: 2004. <http://www.globalsecurity.org/ wmd/library/congress/2004_r/04-07-22emp.pdf> [10 January 2005].

Greer, James K. “Operational Art for the Objective Force.” Military Review, (September-October 2002): 22-29. <http://www.leavenworth.army.mil/milrev/download/ English/SepOct02/greer.pdf> [21 January 2005].

Heylighen, Francis and Cliff Joslyn. “What is Systems Theory?” Principia Cybernetica Web. 01 November 1992. <http://pespmc1.vub.ac.be/SYSTHEOR.html> [22 January 2005].

James, Glenn E. Chaos Theory: The Essentials for Military Applications. The Newport Papers, no. 10. Newport, R.I.: U.S. Naval War College, October 1996.

Kopp, Carlo. A Doctrine for the Use of Electromagnetic Pulse Bombs. Royal Australian Air Force Air Power Studies Centre Working Paper, no. 15 (revised draft). Canberra, Australia: RAAF Air Power Studies Centre, July 1993. <http://www.csse.monash.edu.au/~carlo/archive/MILITARY/ APSC/wp15-draft.pdf> [11 January 2005].

_____. “The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction.” Air & Space Power Chronicles Online Journal. 1996. <http://www.airpower.maxwell.af.mil/ airchronicles/kopp/apjemp.html> [11 January 2005].

_____. “Hardening Your Computer Assets.” 1997 Reports. 22 December 2004. <http://www.globalsecurity.org/military/library/report/1997/harden.pdf> [11 January 2005].

_____. An Introduction to the Technical and Operational Aspects of the Electromagnetic Bomb. Royal Australian Air Force Air Power Studies Centre, no. 50. Canberra, Australia: RAAF Air Power Studies Centre, November 1996. <http://www.csse.monash.edu.au/%7Ecarlo/archive/MILITARY/APSC/wp50-draft.pdf> [11 January 2005].

Lilley, James R. and David Shambaugh, eds. China's Military Faces the Future. Washington, D.C.: American Enterprise Institute, 1999.

People's Republic of China State Council Information Office. "China's National Defense in 2004." Government White Papers. 27 December 2004. <http://www.china.org.cn/ewhite/20041227/index.htm> [20 January 2005].

Respectfully Quoted: A Dictionary of Quotations Requested from the Congressional Research Service. Washington, D.C.: Library of Congress, 1989; New York: Bartleby.com, 2003. <http://www.bartleby.com/73/1240.html> [20 January 2005].

U.S. Congress. House. Committee on National Security, Subcommittee on Military Research and Development. Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure: Hearing before the Military Research and Development Subcommittee. 105th Cong., 1st sess., 16 July 1997. <http://web.lexis-nexis.com/congcomp/ document?_m=03888fa59248169d783c6fa47c458cb5&_docnum=30&wchp=dGLbVtz-zSkSA&_md5=da0fcdd87891abe715592cb51fd15397> [11 January 2005].

U.S. Department of the Army. Maintenance of Mechanical and Electrical Equipment at Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities: System Design Features. TM 5-692-2. Washington, D.C.: 15 April 2001. <http://www.usace.army.mil/inet/ usace-docs/armytm/tm5-692-2/chap27VOL-2.pdf> [11 January 2005].

U.S. Joint Chiefs of Staff. Joint Doctrine for Campaign Planning. Joint Publication 5-00.1. Washington, D.C.: 25 January 2002.

U.S. Office of Force Transformation. The Implementation of Network-Centric Warfare. Washington, D.C.: 2005. <http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf> [15 January 2005].