Recent operational experiences have prompted many military professionals to seek further understanding of the interconnectedness of computer networks and how this understanding can be merged with their existing knowledge of traditional wargfighting skills such as combined arms operations. While requiring significant investment and coordination, the integration of computer network attack into tactical level combined arms operations will significantly increase the effectiveness of U.S. military forces and their ability to succeed in future wars.
FUTURE WAR PAPER

“BEYOND THE BANG: EXPANDING COMBINED ARMS OPERATIONS THROUGH TACTICAL LEVEL APPLICATION OF COMPUTER NETWORK ATTACK”

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF OPERATIONAL STUDIES

AUTHOR: MAJOR B. W. TIPPETT, USMC

AY 2009-10

Mentor: Dr. Gordon Rudd
Approved: 
Date: 27 MAY 2010
DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.
Military planners and strategists throughout the ages have sought ways to wage war with minimal loss to their own nation’s blood and treasure. While many have posited their theories and views on this subject perhaps none is better known than Sun Tzu. Heralding that, “To subdue the enemy without fighting is the acme of skill.”¹ Sun Tzu recognized the value of achieving decisive effects on the enemy before armies met on the field of battle. While organized governments have always had the ability to apply force to achieve decision across what is today commonly refer to as the elements of national power (i.e. diplomatic, information, military, and economic), military professionals have for centuries been almost exclusively confined to the use of force through kinetic means to contribute to the achievement of policy goals. As such, combined arms operations have dominated the schema of modern military professionals.

Rooted in the efficient and effective application of kinetic force, combined arms operations have very seldom sought to integrate an “arm” that was not kinetic. Over the past half century, advances in computer and network technologies have added new dimensions to a military force’s means to exert its will on an adversary. Recent operational experiences have prompted many military professionals to seek further understanding of the interconnectedness of computer networks and how this understanding can be merged with their existing knowledge of traditional warfighting skills such as combined arms operations. While requiring significant investment and coordination, the integration of computer network attack into tactical level combined arms operations will significantly increase the effectiveness of U.S. military forces and their ability to succeed in future wars.
**Current State of Affairs**

Computer Network Attack (CNA), while not an existing part of combined arms operations, is not a new capability within civilian or military realms. Joint Publication 3-13, *Information Operations* defines CNA as those “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves”.² Doctrinally, CNA is a subdivision of Computer Network Operations (CNO). CNO, as one of five core capabilities of Information Operations (IO), integrates with four other core capabilities, psychological operations, military deception, operational security, and electronic warfare along with the related and supporting capabilities to “provide the JFC with the principal means of influencing an adversary or other Target Audiences”.³ Gaining an appreciation for how IO, CNO, and specifically CNA have been approached and applied in military planning and operations to date will provide a better understanding of where they may realistically be expected to be taken in the future.

IO began its doctrinal life within U.S. Joint Operations in 1998 with Joint Publication 3-13, *Information Operations*.⁴ The recognition of the importance of IO by Joint Forces Command indicated the growing dependency of military operations on computer and telecommunication networks.⁵ During this same period military leaders also recognized that it was not the networks or systems themselves that held such importance, but rather the information they carried that was and is of prime importance to the military. Importantly, Joint doctrine also communicated that information itself cannot be attacked or defended, it can be influenced, disrupted, or corrupted.⁶
Since its original and subsequent publication in 2006, Joint Publication 3-13, *Information Operations* has done a marginal job describing and organizing a set of capabilities that are often times viewed as disparate in their nature by the end-user. Organized into core, supporting, and related capabilities, IO has proved hard for most military professionals to conceptualize let alone operationalize. Despite the difficulty in capturing the “what” and “how” of IO, recent operations in Iraq and Afghanistan have demonstrated clearly to military planners and operators alike that there is value in integrating IO into all military operations. However, as a result of poor understanding of how to organize and apply IO, military servicemen have developed a host of disparate methods of implementing IO into operations. Two of the most common include viewing it as a non-doctrinal warfighting function or battlefield operating system or elevating it to an undefined status as something that transcends all warfighting functions or lines of operation as illustrated in Figure 1 taken from Field Manual 3-24, *Counterinsurgency*.

![Figure 1](image-url)
As the military services have struggled to operationalize IO, one of its core capabilities, CNO has experienced similar difficulties, albeit for different reasons. CNO has as its sub-elements CNA, computer network defense (CND), and computer network exploitation (CNE). These capabilities, while easily defined and understood, have not been something that operational or tactical level planners have requested or contemplated how they might be employed in their operations because of the classification and compartmentalization associated with them. For reasons not relevant to this assessment, CND, has commonly been relegated to a separate supporting function to keep military networks secure.

Despite the existing compartmentalization of these capabilities, examination of the definitions of CNA and CNE allows connections with commonly understood warfighting functions or battlefield operating systems. This association will illustrate how they may be better appreciated by military planners. CNA is commonly categorized into two types of attack: attacks against information systems and attacks against infrastructure-control systems. Information systems (e.g. databases or email) as networks are important because of the information they process, whereas infrastructure control systems are those networks that through computer and telecommunication networks physically control devices (e.g. power or water supplies). Attacks against either of these type systems through cyber or kinetic means is defined as CNA. CNE on the other hand are those “enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks”. Assessing these two definitions, logical associations can be made between CNA and the warfighting function of fires and CNE and the warfighting function of intelligence.
Association of these two forms of CNO provides a recognizable means to view CNA’s application in combined arms. Combined arms operations are defined as “the full integration of combat arms in such a way that to counteract one, the enemy must become more vulnerable to another.”¹¹ Both the United States Army and Marine Corps have continually demonstrated their competence in what might be known as “traditional” combined arms operations, however because of a lack of knowledge and understanding of CNA capabilities a significant amount of learning will be necessary in order to build the capability required to effectively use CNA at the tactical level. Some learning has begun as exhibited by actions with the Department of Defense (DoD) over the past decade.

On June 23, 2009 Secretary of Defense Robert M. Gates established U.S. Cyber Command (USCYBERCOM). This move initiated the reconciliation of years of disparate opinions regarding the control of CNO within DoD.¹² USCYBERCOM is now a subordinate unified command under U.S. Strategic Command and is to be commanded by National Security Agency director General Keith Alexander.¹³ While the challenges associated with capability development, integration, and execution that lay ahead for this command are monumental, its establishment is a necessary first step in generating the “cyber capability at the tactical level”¹⁴ called for by General James Cartwright, Vice Chairman of the Joints Chiefs of Staff. To make this capability a reality will require both the building of the capability (i.e. people, training, and equipment) and a thorough understanding and assessment of the advantages and risks associated with employing cyber attack at the tactical level.
Implications – Requirements, Risks, and Advantages

Conducting CNA at the tactical level is a multifaceted problem. Because this assessment does not include the classified aspects of CNA, only broader implications associated with CNA and warfighting in its entirety will be addressed. When CNA is viewed as a type of fires several supporting requirements surface that require either expansion and/or refinement of existing capabilities.

To employ fires effectively in modern military operations requires a functional and efficient targeting process/cycle. Joint Publication 3-0, *Operations* defines the current six step process as one of “selecting and prioritizing and matching the appropriate response to them, considering operational requirements and capabilities.”15 While CNA expands the means of available response, it also creates additional requirements to be successfully integrated into tactical level combined arms operations. Employing CNA as a response to a particular target requires intelligence that can identify sufficient elements of an adversary system. More specifically, intelligence must be produced that allows planners to determine how a particular computer networks can be engaged to produce the desired effects. When seeking to gain this type of intelligence it becomes clear that existing tactical level intelligence capabilities which “were developed to support kinetic attacks”16 are insufficient. This shortfall will require the development of a proper intelligence support capability that can gather and analyze the information required to successfully apply CNA at the tactical level.

Properly focused and resourced intelligence support will also provide the information required by planners and commanders to develop an efficient approval cycle for CNA. This approval cycle, while likely a subordinate element of the afore mentioned targeting cycle, will be
as vital, if not more when attacking computer networks than when attacking targets with conventional munitions. Because civilian computer networks are deeply intertwined with military networks, CNA has blurred the line regarding attack of civilian property and indirect attacks against civilians. This is further complicated when enemy forces (military or not) use civilian networks for command and control or other battlefield functions. This will require an in-depth understanding of the networks attacked and their relation to other networks to enable planners to produce cyber-collateral damage estimates (CDE). These Cyber-CDEs will allow the commander to determine risk and make his decision regarding the employment of CNA as part of his combined armed operations.

Cyber-CDEs can enable a commander to informatively assess risk to unintended targets (i.e. other computer networks or computer controlled infrastructure) and risk to the technological advantage that enables CNA to be a functional capability. Computer networks are inherently interconnected. Because of this, an attack against the portion of the network intended to have a very precise effect may produce “cyber-spillage”, that is unintended consequences on other portions of a network that go beyond the target locale both in time and space. The effects of such unintended consequences will vary in severity and span of the affect. The cyber-spillage of one CNA could serve as the catalyst for a widened conflict if the effects on an unintended group or nation were significantly severe. In counterinsurgency operations (COIN) or stability operations the effects of a CNA could easily create friction amongst the host nation government and the force employing the CNA. While these illustrations depict some of the risks to unintended targets, the risk to maintaining the ability to continue to employ CNA must also be considered prior to employment.
Risk to preserving CNA capabilities involves both the risk to the technological aspects that enable CNA to be used as well as access to a given network that is enabling the attack. An attack against a network can be against either an information system or an infrastructure control system. Regardless of which type of is being conducted, a degree of technological advantage is required to gain access to the targeted network. When that technology is used to access a network it provides an adversary or competitor the opportunity to copy and/or counter the technology. Additionally, most CNAs are launched by identifying and exploiting a vulnerability in the network. These vulnerabilities can range from a programming code error in an operating system to a person who provides physical access to a network. In any case, once that vulnerability is exploited, it is subject to identification by the network owner or administrator which in most cases will result in that gap within the network being closed. Recognizing the importance of all the previously listed risks and requirements there are real advantages to be gained by applying CNA at the tactical level.

Application of CNA at the tactical level can provide distinct advantages to the force conducting operations. Most obvious is that it expands the available means for exerting force or influence on an adversary. Recent operations in support of Operations Iraqi Freedom and Enduring Freedom have demonstrated the value of a military force being able to apply force by other than kinetic means. In the past this has most often come through the use of a combination of IO core, supporting, and related capabilities. Of the thirteen existing capabilities of IO, psychological operations, electronic warfare, combat camera, and civil military operations have been used most regularly during recent operations. While other capabilities of IO have and continue to be used at the tactical level, a host of factors influence the frequency and depth which they are employed. More often than not a lack of knowledge combined with a degree of
specialization or compartmentalization precludes their being factored into tactical planning. With tactical level CNA, planners and operators will have a wider variety of responses from which to choose their means to exert force or influence on their adversary. Having traditionally seen influence exerted via kinetic means, future adversaries will now be faced with a wider range of threat options.

An equally significant advantage provided to tactical forces with CNA is the ability to achieve persistent, non-permanent affects. Kinetic force, as the U.S. military’s primary means of force exertion, brings with it a significant liability (i.e. the permanent nature of its effects). To illustrate this difference consider a military force that has a need to shut off the power of a particular urban center prior to commencing an attack. With kinetic means, the force has the ability to employ some mix of guided munitions with varying levels of precision to destroy some components of the power system, components that will have to be replaced or rebuilt to restore power. Using CNA to accomplish the same objective, a force might conduct an attack against the system controlling the power to the urban center (i.e. an infrastructure control system) which would result in a disruption of the power until such time as the attack is concluded. In this case, restoration of the power is a matter of cessation of the attack rather than reconstruction of the power system. The value of achieving effects without incurring unnecessary infrastructure damage is self-evident and will be of increasing importance in future conflicts where contests are increasingly influenced by domestic and foreign populations.
**Recommendations**

Having briefly assessed both the current state of affairs of CNA and its related components of IO as well as some of the implications associated with its application in future conflict, three recommendations are proposed to increase the effectiveness of CNA at the tactical level: develop enhanced intelligence, apply against vulnerable networks, and ensure timely feedback.

Limited collection assets along with the long lead time associated with intelligence support to CNA provides challenges to developing a tactical level CNA capability. Identification of information requirements for effective CNA will be a first step in determining the necessary enhancements to the existing intelligence capability. Once an understanding of the information requirements has been gained, an examination of how existing intelligence at all levels (i.e. tactical, operational, strategic, and national) can be integrated to provide the intelligence support necessary at the tactical level must be done. This will likely require the development of a tactical intelligence capability that has a specific focus on computer networks with reach-back capabilities to higher level intelligence capabilities. This will not only serve as a method of gaining the required intelligence to support operations, but also as a method to facilitate deconfliction of CNO across the different levels of war.

Recognizing that existing CNO occurs across many different agencies and levels, tactical CNA must be able to work in conjunction with these existing efforts. A large portion of this will be determining what networks are most conducive to attack and least disruptive to on-going CNO. Tactical CNA operations should then most often be applied against “softer” or more vulnerable networks. Such networks will often be operating as part of an open network.
(e.g. the internet). Such attacks will mitigate risk against exposure of friendly attack capabilities through the anonymity offered by these networks.  

The CNO conducted by strategic and national level organizations and agencies are long-term operations that support further CNO efforts, conventional operations, and intelligence operations. Because these effects are to be integrated not only with other elements of IO, but also in the framework of combined arms operations, they must be measurable within a timely manner. This timeliness will facilitate integration of CNA with other fires. In short the effects must be recognized so as to place the enemy in the dilemma of counteracting one effect only to fall subject to another. In conventional operations this may be a set period for which power will be disrupted in a given city, or in the case of CNA supporting COIN, this might be a period of time in which an information system (e.g. email) will be monitored. Regardless of the type of attack, the key consideration is that feedback of effects must be gained so as to achieve combined arms effects.

Conclusion

This brief assessment has illustrated many of the challenges associated with the application of CNA at the tactical level. Recognizing these challenges and the investment and coordination that will be required to overcome them, it is equally clear that the integration of CNA into tactical combined arms operations will increase the effectiveness of U.S. forces. Future conflict, while having an immutable nature, will continue to change in character. As the world continues to build reliance on computer networks, future conflict will require military forces at all levels to be cognizant of their dependence on these networks and to be aware and capable of gaining advantage over their adversary through the use and exploitation of these
networks. To be sure, attacks against computer networks are no panacea for future warfighting. However, when understood and applied in conjunction with existing military capabilities they do offer U.S. forces the potential for increased advantage over future adversaries.

3 *Information Operations*, (2006), x
9 Ibid, 1
14 Miles.
16 Gibson, 1.
17 David Tubbs, Perry G. Luzwick, Walter Gary Sharp, Sr., 9-10
18 William J. Bayles, “The Ethics of Computer Network Attack.” *Parameters* 31, no. 1 (Spring 2001), 54
19 David Tubbs, Perry G. Luzwick, Walter Gary Sharp, Sr., 10-14
20 *Information Operations*, (2006), xi
21 Miles.
Bibliography


