Naval War College
Newport, R.I.

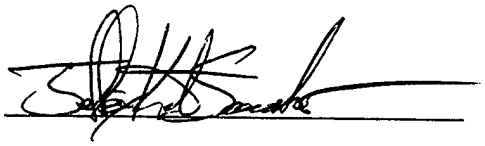
Space, Time and Force: Relationships in Cyber Space

By

Jeffrey K. Souder
Major, United States Army

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



5 February 2001

Advisors:

Faculty Advisor
Roger W. Barnett, Ph.D.
Professor of Naval Warfare Studies

Faculty Advisor
Milan N. Vego, Ph.D.
Professor of Joint Maritime Operations

13 NWCR 98

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): **SPACE, TIME AND FORCE: RELATIONSHIPS IN CYBER SPACE (U)**	
9. Personal Authors: **MAJ JEFFREY K. SOUDER, USA**	
10. Type of Report: FINAL	11. Date of Report: **5 FEB 2001**
12. Page Count: 29	12A Paper Advisor (if any): **PROF BARNETT; PROF VEGO**
13. Supplementary Notation: 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. Ten key words that relate to your paper: **SPACE; TIME; FORCE; CYBER SPACE; INFORMATION OPERATIONS; INFORMATION SUPERIORITY; INTERRELATIONSHIPS; OPERATIONAL FACTORS**	

15. Abstract:

The Joint Chiefs of Staff envision information superiority, attained through the conduct of Information Operations (IO), as key in obtaining full spectrum dominance in future conflicts. Computer Network Attack (CNA) and Defense (CND) are relatively new IO weapons that the operational commander will soon employ along with his other, more traditional, weapons to gain information superiority and maintain freedom of action while limiting that of his enemy. He will also have to defend against the same types of weapons wielded by his enemy, for the depth and breadth of networked computer systems in the U.S. military makes him vulnerable to attack. Planning to execute, and defend against, a CNA is a task not addressed by current planning methodologies and procedures. It will still require the planner to balance the operational factors of space, time, and force in relation to his objective, at times much like he would for a physical attack, and at others, in very new and interesting ways.

16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: C	

Security Classification of This Page Unclassified

Abstract

The Joint Chiefs of Staff envision information superiority, attained through the conduct of Information Operations (IO), as key in obtaining full spectrum dominance in future conflicts. Computer Network Attack (CNA) and Defense (CND) are relatively new IO weapons that the operational commander will soon employ along with his other, more traditional, weapons to gain information superiority and maintain freedom of action while limiting that of his enemy. He will also have to defend against the same types of weapons wielded by his enemy, for the depth and breadth of networked computer systems in the U.S. military makes him vulnerable to attack Planning to execute, and defend against, a CNA is a task not addressed by current planning methodologies and procedures. It will still require the planner to balance the operational factors of space, time, and force in relation to his objective, at times much like he would for a physical attack, and at others, in very new and interesting ways. In the physical world, the factors impose on him certain limits that cannot be denied: a larger physical space takes longer to traverse than a smaller one, a smaller space restricts the movement of a large force, and it takes longer to equip and train a large force than it does a small one. In the context of a CNA however, these three factors mean different things to the planner. Cyber space is defined by the sizes and numbers of the adversary's networked automation systems. Within the cyber space distance is nearly irrelevant, speed is almost instantaneous, and forces are able to "arrive" with little or no warning, strike, and maintain the attack for as long as necessary to attain the objective without experiencing fatigue or injury. Attacks may never even be detected. The planner must understand the operational factors in cyberspace and use their unique interrelationships to his advantage when seeking to gain information superiority.

Preface

The focus of this research paper is on a specific type of attack, itself an element of a supporting operational function. The author does not wish to mislead the reader into thinking that he is proposing that the computer network attack, or that Information Warfare/Command and Control Warfare, for that matter, plays anything but a supporting role within the theater.

Introduction

The Joint Chiefs of Staff, through Joint Vision 2020, call for a "continuing transformation of America's armed forces" in order to prepare them to meet the challenges of an uncertain future. They envision information superiority, attained through the conduct of Information Operations (IO), as both a "key enabler" in the transformation, and as a prerequisite to achieving full spectrum dominance.[1]

Information Operations encompass any actions taken to deny the enemy information while protecting one's own[2] and can be conducted such that the enemy is forced to operate with less information than he requires. An IO conducted during time of conflict is an act of Information Warfare (IW) and can be comprised of both offensive and defensive operations, including electronic warfare, physical destruction, and information attack and defense, among others. Any one of these directed against command and control targets in military operations is a type of Command and Control Warfare (C2W).[3] By denying the enemy C2 information he needs to operate, the commander can tilt the balance of information in his favor and gain "information superiority." Effective C2W can limit or completely deny the enemy the freedom of action while retaining the commander's ability to act as he wishes.

Two new, and potentially powerful, IW/C2W weapons recently made available to the operational level commander are Computer Network Attack (CNA) and Computer Network Defense (CND). U.S. SPACECOM has been tasked to lead development of CNA/CND strategy within the Department of Defense, and will share the execution mission with the Commanders-in-Chief (CINCs) deployed around the world.[4]

Planning for these additions to the CINC's traditional C2W mission, especially that of executing a CNA, is one not specifically addressed in any of the newer or long-standing joint

publications and service-specific doctrinal publications, and is not a part of the planning methodologies and procedures well understood by CINC and operational-level commanders and their staffs. These commanders and staffs will have to apply new and innovative thinking in order to reap the benefits CNA offers them. Planning for CNA should not, however, be an exercise entirely foreign to them, for the goal of the CNA is still to contribute to the denial of the enemy's freedom of action. Planning for effective CNA will still require the planner to balance the operational factors of space, time, and force in relation to his objective; at times much as he would for a physical attack, and at others, in very new and interesting ways.

The intent of this paper is to examine the unique ways space, time, and force interrelate when operational art is applied to the planning of a CNA and to propose ways the planner can use them to his advantage. After a brief discussion of C2W targets and the CNA threat against the U.S., the effect of each of the operational factors separately, and then combined, on planning and execution of a CNA will be examined. The conclusion will contain recommendations as to how the staff can ensure its CNA planning is effective.

CNA as a C2W Weapon

Offensive C2W should impair or destroy targets that influence the adversary's estimate of the situation, his ability to make decisions, disseminate those decisions, or assess the results of those decisions. Doing so tilts the balance of information in favor of the commander and allows him to gain and exploit freedom of action because his decisions are the quicker of the two and are based on better information.[5] Because militaries worldwide are increasingly dependent on networked decision support and command and control systems, the numbers and types of potential C2W targets are increasing. Of the twelve target

sets identified at the start of Operation DESERT STORM,[6] three of them could be classified as C2W targets susceptible to CNA.*

Computer Network Attack (CNA) as a method of C2W holds special value for the CINC or operational level commander. It is cheap, safe, can be executed from remote locations, and quick. Additionally, the nature of CNA makes it very difficult for one's adversary to pin blame or, in many cases, even detect that he has been attacked. Such characteristics allow the commander to take preemptive, precise, and confidential actions that not only assist him in shaping his theater, but also assist in protecting his forces, preparing for future contingencies.

If deterrence fails, CNA is a combat multiplier when sequenced and synchronized with the physical weapons at the commander's disposal. When employed during the war, CNA can amplify the effects of the "fog and friction" of combat experienced by the enemy, and enable the commander to not only dominate the enemy's decision cycle with misinformation and destruction of key C2W assets, but also exploit the opportunities resulting from enemy indecision as they evolve.[7] Although apparently never employed, the JTF commander in Kosovo during NOBLE ANVIL considered employing CNA but refrained due to the uncertainties and limitations surrounding its use.[8] Had he employed CNA, he could have attacked key command and control nodes in Kosovo, networked air defense systems, forward deployed sensors, and even the public telephone network being used for C2 communications.[9]

* Electricity Production Facilities (powering C2 nodes); Telecommunications and Command, Control and Communications Nodes; and the Strategic Integrated Air Defense System.

The Threat

The U.S. military stands out as a target for CNA because it depends on automation for so many of its military weapons, logistics, and command and control systems. The U.S. willingness to quickly adapt the latest technologies and the newest software opens it to bugs and security flaws that allow the entrance of intruders.[10] The reliance on commonly available commercial software means adversaries can easily obtain that same software and experiment in order to find ways to intrude into important systems.

The Chinese People's Liberation Army (PLA) daily newspaper recently hypothesized that "societal paralysis" could result in America if a strategic IW attack hampered U.S. military and civilian communications systems, air traffic control system, financial networks, fuel pipeline pumping software, and computer-based clock/timing systems.[11] PLA representatives have separately stated that China is resolved to protect its information resources and communications systems as necessary.[12] Elsewhere, Israelis and Palestinians are currently waging a cyberwar in support of their ongoing tensions in the Middle East that include system penetrations, information operations, and the possible use of Trojan horse viruses.[13]

Responding to an ever-growing list of such information warfare threats, President Clinton and Secretary of Defense William Cohen last year instructed the military to "gear up to wage cyberwar."[14] In response, SPACECOM is preparing OPLAN 3600 to detail the initiatives SPACECOM and the CINCs will take to combat the cyberwarfare threat.[15] SPACECOM plans to develop new types of CNA weaponry to launch distributed denial of service attacks and computer viruses.[16]

Planning

No matter what specific tools and strategies SPACECOM develops, the commander and his staff will need to apply operational art in planning the CNA in order to ensure it supports the C2W mission. In planning a physical attack, the planner seeks to balance the operational factors of space, time, and force in order to ensure that their interrelationship works to the greatest degree in favor of the commander and does not advantage the enemy. In the context of planning a CNA however, those same operational factors interrelate in sometimes peculiar and interesting ways. The planner should understand and take advantage of them in order to make his plan as effective as possible.

Factor Space

Armies control territory through occupation of land space. In contrast, oceans and airspace are so large that denying access to the space may be is more effective in restricting the enemy's freedom of action and increasing one's own than is trying to control his actions within the space. Cyberspace, the space within which a CNA is conducted, is more like oceans and air than land. The whole of cyberspace cannot be controlled because of its virtual size and the technical limitations of the available tools, but critical parts of it can be denied.

The cyberspace in which the CNA will be conducted will be comprised of a virtual "no man's land" through which friendly, enemy, and neutral packets of data will traverse when moving from their origin to their intended destinations. Some of these areas are merely the router, bridge, and other switching and communication nodes across which the data flows. Other nodes will be the actual data repositories, sensing devices, computers, control devices, and automated tools of war that will become CNA targets. It is through attacking

these targets that the commander can deny parts of cyberspace to the enemy. Safe havens might exist only behind proven firewalls, within systems disconnected from the Internet, and within and between systems tunneled through an existing Internet using network encryption devices, and even these are subject to intrusion. In such an environment, the areas outside one's immediate control are best denied and the areas within one's own perimeter controlled.

Between the safe havens, enemy territories, and "no man's land" there may also exist neutral areas owned by neutral countries. International and customary law may apply in any or all of these areas. For example, The International Telecommunications Satellite Organization Agreement of 1973 seeks to ensure that satellites are used only for peaceful purposes. The agreement does recognize that there are satellite systems which have military missions and exempts them, but the planner must keep in mind that the Department of Defense uses civilian systems to satisfy a large portion of its long-haul communications requirements.[17] The ownership of these satellites and systems may come into play depending on the size of the operation and the belligerents involved. The fundamental issue of whether or not IO that involves "neutral" systems (including parts of the Internet) should be considered as such or as " non-peaceful" has not yet been settled.[18] The cyberwarrior will not be able to tell if, in attacking his chosen target, he has traversed a network owned by a neutral country, and that neutral country will most likely not be able to tell that he has done so. It is just this fact, in itself, that gives so much power to the asymmetric warrior. The cyberspace of a country is easily invaded and detection of an invasion is difficult to detect.[19]

Within cyberspace, the only boundaries are those set to provide protection. The forms of protection can include virtual protection limited by Rules of Engagement (ROE) or law, and automated protection afforded by firewalls, sharing mechanisms, or other such

software. There is also the boundary established by the disconnection of a system or network from the rest of a network. But there are no international, geographic, or theater boundaries. Commanders may find it difficult to determine in which geographic theater his targets are located. Due to the nature of Internet routing protocols and the irrelevance of distance in cyberspace, an attack may traverse or target systems in geographic areas outside of his area of responsibility, and coordination will be required with adjacent CINCs. OPLAN 3600 should address coordination issues such as these.

Distance in this cyberspace is almost entirely irrelevant.[20] Data within the space moves at nearly the speed of light and attack can come from any quarter almost instantaneously after its launch. Assuming the location of a potential target is identified, a probing or collection mission to collect intelligence information can be begun immediately after the intelligence request is issued. Within this space there is no need to plan time for a force to arrive, but at the same time, there is no time to react if intelligence of an attack has been obtained. In fact, in most cases the attack will already be over and the damage done by the time it is identified. This fact alone implies that planning for CNA and CND must be quite different than that of physical attack and defense.

Because distance is irrelevant, position within the space relative to the attacking force is also *nearly* irrelevant. If attackers can maneuver at nearly light speed, positioning an important database in one country or another is relatively meaningless if the only advantage in that positioning is achieving greater geographical distance from the enemy. Defensive positioning is important, however, when planning where that database is located in relation to firewalls, how many entrances there are into the network on which it operates, who controls the network, and who has access. Positioning of highly sensitive information and critical

servers will need to be planned to ensure that the best defense possible can be afforded to that device.

The position chosen from which to launch an attack needs to offer access through public networks, thus making the attack less likely to be traced due to the complexity of the Internet if, in fact, that is the intent. More importantly, the attacker needs to plan to gather the intelligence necessary to execute the attack from an advantageous position. It will be very difficult in this cyber space to find C2W targets, especially if one is trying to be stealthy. Assume for a moment that the target of one's attack is a logistics server reporting theater-wide ammunition quantities at a certain depot. If that server is connected to a publicly accessible network, it will be merely a matter of positioning one's computer at a place it can gain access to that network. Positioning of the attacking computer becomes another matter entirely when the target of an attack is the main computer controlling an automated C2 system. Positioning in that context would require the attacker to gain physical access to what will most likely be a closed network. It is in positioning cases like this where time becomes a factor. Prior placement of a Trojan or a trapdoor* in this situation would make effective attack on that system much easier to execute.

Factor Time

Because of the irrelevance of distance in cyberspace, the speed at which some types of CNA can be executed, across great *virtual* distances, is a significant factor in planning for both the offense and the defense. The enemy sees no warning of an impending attack, no massing of troops, no dusty haze arising along a trail on the horizon indicating the enemy forces are approaching. CNA is just there; it arrives and it is gone. This withering speed of

* See Appendix A

attack is one of the greatest advantages of CNA and the operational commander can use it to his advantage when faced with an unexpected turn of events.

A real-world example in which the speed of a CNA might have been employed to remedy an unexpected situation with some effectiveness occurred in Kosovo during Operation NOBLE ANVIL. "Tail watchers" along the fence line of bases from which allied aircraft flew were discovered to be using the public cell phone networks to alert the Serbian air defense system when to expect enemy air traffic.[21] CNA could have been used to target the local cells and inhibit any calls to Serbia.

As in the physical world, time is of critical importance to the commander planning and executing a CNA. The commander who has a disadvantage in physical force capability, size, training, or readiness, or who is at a disadvantage due to the limitations of the space in which he or his opponent is operating, can seek to overcome these disadvantages by employing his time wisely. A staff that has planned early and well can use flexibility, positioning, and speed to overcome other disadvantages during the operation. Furthermore, if the enemy's ability to sense the current situation accurately is impaired, and the friendly commander can make accurate decisions more quickly, he will have the advantage. The inherent speed of CNA could be used to deliver just such an advantage to the friendly commander, but due its complexity and the precise information required to execute a CNA, a long lead-time is required, in most cases, to plan the attack.[22] It was a lack of such advanced planning and preparation that was responsible, in part, for the delay of the commencement of IO against Serbia during NOBLE ANVIL.[23]

Joint Pub 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace, contains Time Event Matrices that include CNA. Use of such

a matrices can assist the planners in synchronizing and sequencing CNA effectively. For example, in the opening days of the next conflict against an enemy with significant theater air defenses, the commander will most likely seek to neutralize that capability. He may gain an advantage by employing CNA in such a way as to confuse enemy theater-level integrated radar systems just prior to, or as his EW and anti-radar air assets begin their attack -- much like was done during DESERT STORM by tapping into enemy phone lines -- but without risk to his soldiers.[24] The same was accomplished during NOBLE ANVIL by using aircraft.[25] The commander might look to CNA to confuse the enemy Air Defense Artillery (ADA) system by clogging the control computer with bogus tracks, his communications assets could be overloaded with misleading data, or his guidance control computers could be infected with a virus that disables them. If the ADA system were emplaced and running off of commercial power, an indirect CNA attack on the power grid, if synchronized properly, could gain an advantage for the attack.

When planning an attack, the commander needs to determine whether he wishes the enemy to know who is responsible for the attack, as well as whether or not he even wants the enemy to know he has been attacked. In some situations, he will want the attack to be brief enough to be effective but not detected or tracked; in others, he may want the attack to be of a duration that denies use of a certain C2 system to the enemy for a longer period of time.

The duration of the attack is an aspect of CNA in the context of time that is quite different from that of a physical attack because CNA does not necessarily require humans to execute. An automated CNA can be designed such that the attack moves from target to target with speed and agility not possible in the physical war, and for durations not possible with attacks conducted by soldiers.

Factor Force

In the physical world, the commander is used to looking for certain indicators of a potential operation: movement, arms buildup, an increased rate of spending for supplies and arms, radar signatures, increased radio communications, or any one of a number of other indicators. Forces can detect an impending attack through the use of such methods as satellite imagery, electronic intelligence, and conventional observation and reporting. Such is not the case with CNA. Unless each automated system and the network to which it is connected is being actively monitored on a continuous basis, an attacker can enter, commit CNA, and leave without ever being detected and possibly leaving no trace the attack occurred. And even such continuous monitoring does not protect one from the danger of trap doors built into the system's operating system or applications, the existence of a Trojan horse virus which has yet to be identified by the makers of anti-virus software, or the lasting effects of misleading data buried deep within a database. As briefly addressed earlier, the friendly force preparing for and then conducting a CNA might not be detected by the enemy until it is too late. In fact, they might never be detected and it is possible to predict that in many cases, attribution for the attack will not be possible.

The same facts apply to the commander's ability to detect a possibly devastating attack from his enemy. As the U.S. comes to rely increasingly on automated and networked information systems, "the value of maintaining and securing them rises. Conversely, the value to an adversary of gaining access to the system, denying service and corrupting its contents, also rises."[26] Assuming the low-budget attacker can gather intelligence about potential targets and the effects of taking out those targets in a stealthy manner, there is really

no way the commander can detect an impending CNA. This fact alone makes the U.S. very vulnerable to the asymmetric attack. The planner must keep in mind that there is really no relationship between the size of the attack (or attacker, his nation, or his military) and either the objective or the impact caused by neutralizing or destroying the objective.

Thinking along these same lines, one can see how in CNA, limited to the confines of cyberspace, the strength of advantage falls naturally to the attacker in ways Clausewitz could never have foreseen when he described the overwhelming superiority of the defense.[27] Current technology allows an attacker to move about within one's cyberspace undetected, leisurely mapping the space, noting locations of devices and information committing an attack if desired and then withdrawing with little trace of his visit. Most intrusion detection systems are only employed at the gateway of a network; and once inside, an attacker can operate without being disturbed. It is for this reason that the best defense might be an active offense.[28]

The C2 targets against which the planner can execute a CNA are many and varied and need to be such that their destruction or degradation supports the commander's objectives for the mission, and does not break international law or the ROE established for the operation. Unlike physical attacks on targets, it is no longer necessary to actually cause destruction of the target. For example, it may be effective enough to target the computer network controlling power generation facilities that support the enemy command and control facilities, vice the facilities themselves.[29] Assuming an attack and its effects have been well-planned and researched, it is also important to realize that crippling a system's ability to provide service is not necessarily as damaging to the adversary as is corrupting information and the decisions that depend on it.[30] For just such reasons, the planner may, at times, wish

not to reveal himself or his attack and continue to corrupt the opposing forces' decisions through misinformation management.

Factor Space Related to Time

Within this space, the defender cannot trade space for time. Because distance is nearly irrelevant, any space the defender might trade would buy him nothing anyway, unless he is trading efficiency for security, i.e. he is positioning critical information off of an easily accessed network to ensure it is secure, or he is keeping critical control systems "unplugged" from the network for the same reasons. But this is not really trading space for time because if the attacker has forced the defender to discontinue use of the system, he has denied it.

Factor Space Related to Force

The inversely proportional relationship between space and the combat power due to a military's use of automation is an interesting one to examine. The more a commander relies on networked automation to support his operational functions, the more susceptible his force is to CNA launched by his adversary. In other words, the larger the cyberspace created by these networked computing systems is, the larger the space his enemy has in which to gather intelligence, the greater the number of targets, and the harder it is to defend.[31] Conversely, that greater space will make finding a particular target more difficult for the enemy.

Within a larger cyber space, the attacker can maneuver to find weaknesses, high-value targets, and evidence of physical world activities. The same space helps the defender only by providing him with more places to confuse his attacker, hide important data, and plant honey pots. In cyberwar, until technology provides the defender a way to maneuver to

defeat a CNA, the space created by the automated systems definitely favors the attacker simply because the defender must employ either a static defense or go on the offense. In contrast, however, these same networked automated systems give the owner greater combat effectiveness in the physical world.

For the same reasons, a commander with fewer networked automation capabilities will have less cyberspace to protect, less risk will be incurred by keeping his systems networked, and that cyberspace created by those systems will be easier to protect. It can also be said that an intrusion into that smaller friendly cyberspace will be easier to detect. Fewer gateways into and out of the network certainly make defense much easier. Thus, it may be difficult to retaliate against an asymmetric attacker using CNA.

Factor Time Related to Force

The attacker's ability to emplace CNA weapons effectively depends upon the complexity of the opponent's defense, the breadth and depth of his automated systems, and the amount of intelligence the commander possesses regarding those systems. The preparation of tailored tools* that can assist in gathering that intelligence takes time and must be planned as well. The size of the enemy's force and the size of one's own, measured both in numbers of humans as well as numbers of automated tools and systems, will determine how much time is needed to prepare adequately. It will require time to map the enemy's cyber space so that the planners can find the targets they need when the time comes to attack. Certain types of active cyber weapons† may have to be put in place long before they are needed. Other types of attacks that deny service to database servers, destroy automated

* See Appendix A
† See Appendix B

control of weapons and command and control systems, or employ viruses to disable sensors, for example, can be effective almost as soon as they are employed, and can provide great advantage to the commander if synchronized and sequenced as a part of his overall plan.

The Interrelationship of Space, Time and Force

To this point it has been established that cyber space is defined by the sizes and numbers of the adversary's networked automation systems connected by neutral territories and "no man's land." Within the cyber space distance has been termed nearly irrelevant, speed almost instantaneous, and forces able to "arrive" with little or no warning, strike, and maintain the attack for as long as necessary to attain the objective. It is interesting to examine how these three factors interrelate through the example of a scripted* C2W CNA in which the attack is run entirely in an automated fashion.

Targets must be selected well in advance, and the intended effects of the attack well understood in order to ensure maximum effect and minimal collateral damage. A script must be developed as an integrated part of the commander's plan to execute a series of sequenced CNAs on widely varying targets all linked to, and affecting, the enemy command and control system. This takes time, but can be done far from the battlefield. The script would begin executing in synchronization with the physical attacks. Relatively few operators would monitor the script, do what damage assessment they could as the attack progresses, and monitor the physical attack in order to maintain synchronization with it. The script could release or initiate viruses, start programs to simultaneously enter multiple enemy systems through trapdoors, transmit bogus data, overload nodes, and deny networks.† Meanwhile, the

* A "script" can be likened to a simple program designed to execute sub-programs in a certain order.
† See Appendix A

enemy defenders of the attack, since they could not have prepared a defensive script to counterattack the friendly one, would never know where the attack was taking place. The enemy commander would lose command and control systems to physical attack and not know if he could trust the ones that remained. More importantly, his response could be shaped[32] if the script was designed to affect those remaining C2 systems in subtle ways that benefited the friendly commander.

The intent of this hypothetical example is to show that if significant time is spent in preparation, the commander can execute a C2W CNA that moves from target to target with withering speed, with no warning, and with almost no human force involvement. In doing so, he has leveraged the time, space, and force relationship peculiar to CNA because he has forced his opponent to expend troops and time in response to an action in which he did not. He has attacked from a great distance instantaneously, with no warning, with cost in fuel or provisions, and with no fatigue risk to his forces. He inhibited enemy C2 and blinded and confused the enemy, thus restricting freedom of action. In Kosovo, NATO forces experienced such confusion and it resulted in wasted munitions and inaccurate situation and battle damage assessments.[33] To counter such an attack, his opponent would have to commit significant physical forces to defend such a swift and wide-ranging attack and would have to take systems "offline" in order to make repairs or guard them against attack – resulting in denial. Unlike physical damage, CNA damage could be transparent to the enemy if selected files were altered during the attack, new viruses were planted, and new intelligence gained. The cost of repair in time and force to the enemy will be much greater than that used by the commander to plan and prepare the attack.

Conclusion

The three operational factors are as inextricably linked in the context of CNA as they are in the context of a physical attack, but in quite different ways. The CNA planner can leverage this skewing of the relationships to his advantage. Physically, a commander must balance space, time, and force in relation to his objective in order to obtain and maintain freedom of action. These factors impose on him certain limits that cannot be denied: a larger physical space takes longer to traverse than a smaller one, a smaller space restricts the movement of a large force, and it takes longer to equip and train a large force than it does a small one. In the context of a CNA however, these three factors mean different things to the planner. Cyber space is defined by the sizes and numbers of the adversary's networked automation systems connected by neutral territories and "no man's land." Within the cyber space distance is nearly irrelevant, speed is almost instantaneous, and forces are able to "arrive" with little or no warning, strike, and maintain the attack for as long as necessary to attain the objective without experiencing fatigue or injury. The planner who understands the operational factors in cyberspace can use their interrelationships to his advantage in attaining his C2W objective.

Recommendations

The planner must:

- Possess comprehensive intelligence regarding his targets.
- Plan well in advance of the intended operation for increased effectiveness.
- Train to ensure an understanding of the operational factors in the CNA context and the implications of their interrelationships.
- Understand the U.S. vulnerability to attack and plan to ensure a robust defense.

Notes

[1] "Joint Vision 2020," June 2000, Joint Electronic Library CD-ROM, Washington, DC: Joint Chiefs of Staff, August 2000.

[2] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), I-1.

[3] Ibid., I-4.

[4] Ellen Messmer, "U.S. Army Kick-Starts Cyberwar Machine," Network World Fusion, 22 November 2000, < http://www.nwfusion.com/news/2000/1120cyberattack.html > [27 December 2000].

[5] Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare, Joint Pub 3-13.1 (Washington, DC: 7 February 1996), vi.

[6] Department of Defense, Conduct of the Persian Gulf War – Final Report to Congress (Washington, DC: 1992), 126-130.

[7] George J. Stein, "Information War - Cyberwar – Netwar," Battlefield Of The Future - 21st Century Warfare Issues, 22 December 1998, <http://www.airpower.au.af.mil /airchronicles/battle/chp6.html > [29 December 2000].

[8] "U.S. - Military Struggles With Rules Of Cyber Warfare," Washington Post, 8 November 1999, Daily Defense News, Periscope, Rockville, MD: Periscope, (27 December 2000).

[9] Kernan Chaisson, "Cyber Warfare Rules 'Bumfuzzle' DOD Lawyers," Journal of Electronic Defense, January 2000, ProQuest, Ann Arbor, MI.: Bell & Howell Information and Learning Company, (27 December 2000).

[10] Martin C. Libicki, "Information War, Information Peace," Journal of National Defense, Spring 1998, ProQuest, Ann Arbor, MI.: Bell & Howell Information and Learning Company, (27 December 2000).

[11] Stein.

[12] Stephen Willingham, "China Plans To Bolster Information Security Efforts, Attaché Says," National Defense, January 2000, ProQuest, Ann Arbor, MI.: Bell & Howell Information and Learning Company, (27 December 2000).

[13] Carmen J. Gentile, "Hacker War Rages in Holy Land," Wired News, 8 November 2000, <http://www.wired.com/news/politics/0,1283,40030,00.html> [27 December 2000].

[14] Messmer.

[15] ibid

[16] ibid

[17] Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force," Naval War College Review, Spring 1998, <http://www.nwc.navy.mil/press/Review/1998/spring/art1-sp8.htm> [27 December 2000].

[18] Ibid.

[19] Julia Allen and others, "State of the Practice of Intrusion Detection Technologies," January 2000, http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028exsum.html> [27 December 2000].

[20] Bruce D. Berkowitz, "War Logs On - Girding America for Computer Combat," Foreign Affairs, May 2000, Military Library FullTEXT, Boston, MA.: EBSCO Publishing, (27 December 2000).

[21] Chaisson,

[22] Berkowitz.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Libicki.

[27] Michael I. Handel, Masters of War: Classical Strategic Thought, 2nd ed. (London: Frank Cass & Co. Ltd., 1996), 96.

[28] "U.S. Space Command Takes Charge Of Computer Network Attack," 29 September 2000, < http://www.peterson.af.mil/usspace/rel15-00.htm> [28 December 2000].

[29] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 19 November 1999, <http://www.usafa.af.mil/iita/assets/images/FNLSCHM.doc> [29 December 2000].

[30] Libicki.

[31] Ibid.

[32] Ibid.

[33] Timothy L. Thomas, "Kosovo And The Current Myth Of Information Superiority," Parameters, Spring 2000, ProQuest, Ann Arbor, MI.: Bell & Howell Information and Learning Company, (27 December 2000).

Bibliography

Adams, James. The Next World War – Computers Are the Weapons and the Front Line is Everywhere. New York: Simon & Schuster, 1998.

Alberts, David S., John J. Gartska, and Frederick P. Stein. Network Centric Warfare – Developing and Leveraging Information Superiority. 2nd ed. Washington, DC: Department of Defense C4ISR Cooperative Research Program, 1999.

Allen, Julia, Allan Christie, William Fithen, John McHugh, Jed Pickel, and Ed Stoner. "State of the Practice of Intrusion Detection Technologies." January 2000. <http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028exsum.html> [27 December 2000].

Arquilla, John, David Ronfeldt, and Michele Zanini. "Networks, Netwar, and Information Age Terrorism." The Changing Role of Information in Warfare, edited by Zalmay M. Khalilzad and John P. White, 75-112. Santa Monica, CA: RAND, 1999.

_____. The Advent of Netwar. Santa Monica, CA: RAND, 1996.

Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force." Naval War College Review. Spring 1998. <http://www.nwc.navy.mil/press/Review/1998/spring/art1-sp8.htm> [27 December 2000].

Berkowitz, Bruce D. "War Logs On - Girding America for Computer Combat." Foreign Affairs. May 2000. Military Library FullTEXT. Boston, MA: EBSCO Publishing. (27 December 2000).

Boll, Kenneth. "Like a Lightning Bolt – Information Warfare." Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA: 1999

Campen, Alan D. and Douglas H. Dearth, ed. Cyberwar 2.0: Myths, Mysteries and Reality. Fairfax, VA: AFCEA International Press, 1998.

Chaisson, Kernan. "Cyber Warfare Rules 'Bumfuzzle' DOD Lawyers." Journal of Electronic Defense. January 2000. ProQuest. Ann Arbor, MI: Bell & Howell Information and Learning Company. (27 December 2000).

Dekker, Marcel. "Security of the Internet." The Froehlich/Kent Encyclopedia of Telecommunications. February 1998. <http://www.cert.org/encyc_article/tocencyc.html> [3 January 2001].

Denning, Dorothy E. Information Warfare and Security. Reading, MA: Addison – Wesley, 1999.

Department of Defense. Conduct of the Persian Gulf War – Final Report to Congress. Washington, DC: 1992.

Elam, Donald E. "Attacking the Infrastructure: Exploring Potential Uses of Offensive Information Warfare." Unpublished Research Paper, U.S. Navy Naval Postgraduate School, Monterey, CA: 1996.

Forno, Richard and Ronald Baklarz. The Art of Information Warfare. Parkland, FL: Universal Publishers, 1999.

Gentile, Carmen J. "Hacker War Rages in Holy Land," Wired News. 8 November 2000. <http://www.wired.com/news/politics/0,1283,40030,00.html> [27 December 2000].

Handel, Michael I. Masters of War: Classical Strategic Thought. 2nd ed. London: Frank Cass & Co. Ltd., 1996.

Hosmer, Stephen T. "The Information Revolution and Psychological Effects." The Changing Role of Information in Warfare, edited by Zalmay M. Khalilzad and John P. White, 217-251. Santa Monica, CA: RAND, 1999.

Joint Chiefs of Staff. "Joint Vision 2020." June 2000. Joint Electronic Library CD-ROM. Washington, DC. August 2000.

Libicki, Martin C. "Information War, Information Peace." Journal of National Defense, Spring 1998. ProQuest. Ann Arbor, MI.: Bell & Howell Information and Learning Company. (27 December 2000).

Messmer, Ellen. "U.S. Army Kick-Starts Cyberwar Machine." Network World Fusion. 22 November 2000. < http://www.nwfusion.com/news/2000/1120cyberattack.html > [27 December 2000].

Mollander, Roger C., Peter A.Wilson, and Robert H. Anderson. "U.S. Strategic Vulnerabilities: Threats Against Society." The Changing Role of Information in Warfare, edited by Zalmay M. Khalilzad and John P. White, 253-281. Santa Monica, CA: RAND, 1999.

Nichiporuk, Brian. "U.S. Military Opportunities: Information Warfare Concepts of Operation." The Changing Role of Information in Warfare, edited by Zalmay M. Khalilzad and John P. White, 179-215. Santa Monica, CA: RAND, 1999.

Newmann, Herb W. "Digital Data Warfare Tools: Should CINCs Have Control?" Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA: 1999.

Ochmanek, David A., Edward R. Harshberger, David E. Thaler, and Glenn A. Kent. To Find, And Not To Yield. Santa Monica, CA: RAND, 1998.

O'Connell, Edward P. "Off the Trodden Path: Thinking Through the Military Exploration of the Information Domain." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1997.

Pears, Andrew H. "Planning for the Information Campaign." Unpublished Research Paper, U.S. Air Force Institute Of Technology, Wright-Patterson Air Force Base, OH: 1996.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." 19 November 1999. <http://www.usafa.af.mil/iita/assets/images/FNLSCHM.doc> [29 December 2000].

Stein, George J. "Information War - Cyberwar – Netwar." Battlefield Of The Future – 21st Century Warfare Issues. 22 December 1998. <http://www.airpower.au.af.mil/airchronicles/battle/chp6.html > [29 December 2000].

Thomas, Timothy L. "Kosovo And The Current Myth Of Information Superiority." Parameters. Spring 2000. ProQuest. Ann Arbor, MI: Bell & Howell Information and Learning Company, (27 December 2000).

Treadwell, Mark B. "When Does an Act of Warfare Become an ACT of War? Ambiguity in Perception." Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA: 1998.

U.S. Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare. Joint Pub 3-13.1. Washington, DC: 7 February 1996.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington, DC: 9 October 1998.

"US - Military Struggles With Rules Of Cyber Warfare." Washington Post. 8 November 1999. Daily Defense News. Periscope. Rockville, MD: Periscope. (27 December 2000).

"U.S. Space Command Takes Charge Of Computer Network Attack." 29 September 2000. < http://www.peterson.af.mil/usspace/rel15-00.htm> [28 December 2000].

White, Kenneth C. "Cyber-Terrorism: Modem Mayhem." Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA: 1998.

Willingham, Stephen. "China Plans To Bolster Information Security Efforts, Attaché Says." National Defense. ProQuest. Ann Arbor, MI.: Bell & Howell Information and Learning Company. (27 December 2000).

Appendix A Example Computer Network Attack Techniques*

Account Compromise

An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft, or theft of services. The lack of root-level access means that the damage can usually be contained, but a user-level account is often an entry point for greater access to the system.

Denial of Service

The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

Exploitation of Trust

Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

Malicious Code

Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

Internet Infrastructure Attacks

These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and can seriously hinder the day-to-day operation of many sites.

---

* Marcel Dekker, "Security of the Internet," The Froehlich/Kent Encyclopedia of Telecommunications, February 1998, <http://www.cert.org/encyc_article/tocencyc.html> [3 January 2001}.

Appendix A Example Computer Network Attack Techniques, cont'd

Trapdoor
Legitimate or illegitimate routine designed into application code which allows a software maintainer or attacker to bypass system security safeguards and access the code directly. A way around log on procedures, passwords, and other protection. Can be used by an attacker to manipulate the code, data, or even an operating system.

Bots
Active software "agents" that patrol the Internet collecting information about a specific type of target, such as email addresses or server addresses.

Honey Pots
Sites intentionally left accessible to enemy attackers in order to deceive them into thinking they are attacking valuable sites.

Appendix B Example Computer Network Intelligence Gathering Techniques*

Probe
A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. One example is an attempt to log in to an unused account. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry.

Scan
A scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a misconfiguration or other error, but they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.

Packet Sniffer
A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require privileged access.

Mapper
Collects IP routing information in an attempt to "map" servers acting as gateways to networks, redundant networks, etc.

Bots
Active software "agents" that patrol the Internet collecting information about a specific type of target, such as email addresses or server addresses.

Honey Pots
Sites intentionally left accessible to enemy attackers in order to deceive them into thinking they are attacking valuable sites.

---

* Marcel Dekker, "Security of the Internet," The Froehlich/Kent Encyclopedia of Telecommunications, February 1998, <http://www.cert.org/encyc_article/tocencyc.html> [3 January 2001}.