**Abstract**

The characteristics of cyberspace operations in the future will provide military planners with unique battle space shaping tools, including cyber-reconnaissance; cyber-isolation; and cyber-strike. When these tools are employed in conjunction with other war fighting functions, the conduct of future campaigns will be greatly enhanced.

**Subject Terms**

Cyber, Cyberspace, Planning, Offensive, Cyber-reconnaissance, Cyber-isolation, Cyber-strike, Future, Networks
## INSTRUCTIONS FOR COMPLETING SF 298

| 1. REPORT DATE. | Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998. |
| 2. REPORT TYPE. | State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc. |
| 3. DATES COVERED. | Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998. |
| 4. TITLE. | Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses. |
| 5a. CONTRACT NUMBER. | Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169. |
| 5b. GRANT NUMBER. | Enter all grant numbers as they appear in the report, e.g. 1F665702D1257. |
| 5c. PROGRAM ELEMENT NUMBER. | Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234. |
| 5d. PROJECT NUMBER. | Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR. |
| 5e. TASK NUMBER. | Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112. |
| 5f. WORK UNIT NUMBER. | Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105. |
| 6. AUTHOR(S). | Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr. |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). | Self-explanatory. |
| 8. PERFORMING ORGANIZATION REPORT NUMBER. | Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2. |
| 9. SPONSORING/MONITORS AGENCY NAME(S) AND ADDRESS(ES). | Enter the name and address of the organization(s) financially responsible for and monitoring the work. |
| 10. SPONSOR/MONITOR'S ACRONYM(S). | Enter, if available, e.g. BRL, ARDEC, NADC. |
| 11. SPONSOR/MONITOR'S REPORT NUMBER(S). | Enter report number as assigned by the sponsoring/monitoring agency, if available, e.g. BRL-TR-829; -215. |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT. | Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information. |
| 13. SUPPLEMENTARY NOTES. | Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc. |
| 14. ABSTRACT. | A brief (approximately 200 words) factual summary of the most significant information. |
| 15. SUBJECT TERMS. | Key words or phrases identifying major concepts in the report. |
| 16. SECURITY CLASSIFICATION. | Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page. |
| 17. LIMITATION OF ABSTRACT. | This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited. |
FUTURE WAR PAPER

SHAPING THE FUTURE BATTLESPACE:
OFFENSIVE CYBER WARFARE TOOLS FOR THE PLANNER

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

MAJOR N.P. ROSE
AUSTRALIAN ARMY

AY 2012-2013

Mentor: Dr Bradley Meyer, Ph.D., Professor of Military History
Approved: Bradley J. Meyer
Date: 17 May 2013
DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HERIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF THE MARINE CORPS SCHOOL OF ADVANCED WARFIGHTING, THE AUSTRALIAN DEFENCE FORCE, OR ANY OTHER UNITED STATES OR AUSTRALIAN GOVERNMENT AGENCY.

REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATIONS FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>THE CURRENT UNDERSTANDING OF CYBERSPACE FOR DEFENSE OPERATIONS</td>
<td>2</td>
</tr>
<tr>
<td>OBSERVATIONS ON RECENT CYBER OPERATIONS</td>
<td>3</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>4-5</td>
</tr>
<tr>
<td>Isolation</td>
<td>6-7</td>
</tr>
<tr>
<td>Strike</td>
<td>8-9</td>
</tr>
<tr>
<td>CONSIDERATIONS FOR THE PLANNER IN THE USE OF FUTURE CYBER SHAPING TOOLS</td>
<td>10-14</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>15</td>
</tr>
<tr>
<td>ENDNOTES</td>
<td>16</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>19</td>
</tr>
<tr>
<td>APPENDICIES</td>
<td>23-25</td>
</tr>
</tbody>
</table>
INTRODUCTION

"Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon."

General Hayden, 2011, On Cyberwar development

"The trick to forgetting the big picture is to look at everything close-up."


What does cyberspace offer to strategists in the conduct of future war? Determining an answer to this question is vital. All too often, planners and commanders become entangled with the tactical details of cyber – the ‘ones and zeros’ – without considering more enduring concepts for operational employment. The characteristics of cyberspace operations in the future will provide military planners with unique battle space shaping tools, including cyber-reconnaissance; cyber-isolation; and cyber-strike. When these tools are employed in conjunction with other war fighting functions, the conduct of future campaigns will be greatly enhanced.

Now and increasingly in the future, cyber-reconnaissance will provide planners with enhanced abilities to understand, observe and determine enemy systems’ vulnerabilities, strengths, and how the enemy is using information, particularly in relation to command and control systems. Through enhanced knowledge of an adversary, planners will employ cyber-isolation tools, such as electronic blockades, information manipulation, and computer system denial, independently or in conjunction with traditional war fighting tools. Cyber-isolation will also contribute to the fracturing of alliances and disruption of other elements of national power, such as economic systems. Cyber-strike – a tool to be employed judiciously - will attack with precision specific enemy nodes, systems and infrastructure causing physical effects, that will in many cases overcome traditional physical security and defense mechanisms. To realize the potential of these three future cyber shaping tools, planners must work intimately with cyber-specialists, be educated on the topic of cyber, and finely attuned to cybers unique application.
This paper will discuss and outline the unique characteristics of cyberspace operations that have been exploited in recent operations and that are relevant to planners, including attribution, time, speed, risk, precision and its ephemeral nature. To support the discussion, examples will be used to draw out the emerging operational shaping tools of cyber-reconnaissance, isolation and strike for planners that have future application. Finally, planning considerations for employing the tools at the strategic and operational levels of war will be proposed.

THE CURRENT UNDERSTANDING OF CYBERSPACE FOR DEFENSE OPERATIONS

Definition. Cyberspace as a domain of war fighting has been emphasized by the U.S. government in *U.S. DoD Strategy for Operating in Cyberspace* (2011). The strategy highlights the critical nature of cyberspace for military operations and defines cyberspace as:

“A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

Threats. U.S. Cyber Command categorizes cyber threats into those originating from non-nation state groups (such as terrorist organizations, political organizations, organized hackers, individuals); nation states (such as high level technical cyber attacks often termed ‘Advanced Persistent Threats (APT)’); virtual threats (non-kinetic and online); and physical threats to networks. According to the U.S. Director of National Intelligence, cyber threats broadly consist of cyber-espionage (accessing sensitive information) and cyber-attack (a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt or delete data).

Conceptual. The conceptual understanding of cyberspace is progressing along two broad lines. Firstly, defensive cyber and secondly, offensive cyber. Defensive cyber is aimed at stopping cyber attacks focused on gaining access to information and friendly systems and receives considerable attention; it has been the impetus for establishing organizations such as
U.S. Cyber Command. Offensive cyber, while less developed, is aimed in two directions: response to cyber attacks and the conduct of pro-active virtual activities to enable military operations.

The U.S. has defined offensive cyber operations as:

"...the creation of various enabling and attack effects in cyberspace, to meet or support national and combatant commander's objectives and to actively defend DOD or other information networks, as directed."10

From this definition offensive cyber operations can be ‘active defense’ and/or enabling and attack effects. ‘Active defense’ is well developed due to its close alignment to defensive cyber. The same cannot be said for ‘enabling and attack effects’ in offensive cyber. This aspect of offensive cyber is closely guarded in terms of classification, sensitivity and authorization for use and requires significant reconnaissance, resources and skilled personnel to craft weapons to exploit enemy system’s weaknesses. Yet enabling and attack effects could be extremely useful for the military planner if suitable cyber tools were available.

**OBSERVATIONS ON RECENT CYBER OPERATIONS**

**Reconnaissance.** In 2003 the world was made aware of alleged Chinese ‘viewing’ and ‘borrowing’ of information from nations around the globe under the names of TITAN RAIN and NIGHT DRAGON.11 What was this information used for? Has it been used or stored for use at a later stage? This is an example of reconnaissance being conducted in the realms of cyberspace.

The conduct of general reconnaissance is necessary to understand an adversary.12 The conduct of cyber-reconnaissance is necessary to determine an adversary’s network or system; the system’s weaknesses; its defense mechanism; and who is operating in the system. For the operational planner knowing what is occurring inside the enemy’s computer systems is a vital enabler that should be exploited for advantage.
The alleged activities carried out by the Chinese and other nation states have been labeled in security organizations as ‘Advanced Persistent Threat (APT)’. APT describes high-end state sponsored cyber attacks that are the product of many months or years of cyber-reconnaissance. The intention, as evidenced in recent security analysis of attack trends, has been to gain and maintain access to targeted systems to steal information and use that information for national objectives. A particular aspect observed has been the ability of organizations to maintain access to the targeted system to return at a later date to obtain additional data and remain undetected by the target. Such reconnaissance has usually involved a group or an individual gaining access to protected information. The techniques used by hackers (state or individual) are a component of cyber-reconnaissance (appendix A refers).

APT has military implications. The use of computers has pervaded every aspect of most militaries; while it can give strength to a force it can provide a weakness. The application of cyber-reconnaissance becomes paramount to determine the vulnerabilities in an adversary use of computers during peace and in times of war.

The conduct of cyber reconnaissance of Syrian networks, as a component of the 2007 Israeli Defense Forces Operation ORCHARD (bombing of a suspected nuclear site) determined weaknesses. Identification of weaknesses later enabled the alleged employment by Israeli forces of sophisticated computer code to control it’s air defense systems, deceiving radar operators as to the true air threat picture. This cyber-reconnaissance enabled action, effectively neutralized Syrian air defense systems, allowing the safe passage of Israeli strike aircraft. The employment of deception and information alteration within the adversary system shaped Operation ORCHARD and provides a suitable example of successful cyber reconnaissance.
The alleged activities of China and Israel provide five characteristics of cyber-reconnaissance. Firstly, the nature of cyber-reconnaissance is different from traditional reconnaissance:

"...in no other military endeavor is intelligence so integral to warfighting. But the nature of the reconnaissance is not simply to observe and report. The real purpose of cyberspace reconnaissance has a more scientific bent—to examine a logical structure and determine its flaws, either by observation or by experimentation."\(^\text{17}\)

Secondly, it is extremely difficult to determine who is conducting cyber-reconnaissance, and therefore who is a potential adversary. Attribution of APT to nations such as China cannot be conclusively proven due to Internet routing, employment of multiple servers around the globe and no official claims of responsibility.\(^\text{18}\)

Thirdly, accessing a target system, though cyber-reconnaissance takes time to develop and access requires specialized skill sets to be effective. Fourthly, cyber-reconnaissance can provide unique insight into an adversary that may be cheaper, less risky and unobtainable from other intelligence sources.

Using information gleaned through cyber-reconnaissance, however, is a two-edged sword; if you act on the information collected you may lose access to the systems you invested time and resources to infiltrate.

The use of ULTRA communications intercepts during World War II is an example of weighing the costs against the benefits of acting on information sourced during cyber-like reconnaissance.\(^\text{19}\) The Allied ability during the war to read coded German communications was of immense value to planners and commanders, but decisions on how best to employ that knowledge without its compromise had to be made. ULTRA was able to provide significant support to deception operations, detailed awareness of German orders of battle and intentions (resulting in accurate assessments of capabilities), and influence on Allied strategy. It was however not always complete, as shown by enemy actions, necessitating supplementation by
other forms of intelligence. In the same way, cyber-reconnaissance will likely provide similar functions to future planners.

Finally, the constant and increasing use of cyber systems by global militaries and communities provides more opportunities for information exploitation through the gathering of cyber intelligence that can shape and influence the conduct of military operations. Military planners of the future must consider the use of cyber-reconnaissance as a tool that will complement the shaping of a military operation.

Isolation. Three weeks prior to Russian maneuvers towards Georgia in August 2008 it is alleged that pro-Russian cyber-hackers overloaded Georgian Internet service providers, defaced Georgian government websites with anti-Georgian propaganda and conducted distributed denial of service (DDOS) attacks against government and media websites. Georgia’s ‘cyber’ utilities were being isolated and targeted in preparation for what was to come as part of the Five Day War. At the commencement of Russian land operations in Georgia, cyber-hacking continued with the list of targets increasing to include financial, business, educational and western media outlets. It is reported that Russian hackers isolated media and government communications sites in specific areas in which military attacks were to take place. Additionally, cyber attacks were restricted against infrastructure that would have caused injury or mass chaos in Georgia. The effect of these actions was to isolate both the Georgian government and people from internal and external communications. Through this isolation, the Russian government was able to degrade significantly the Georgian government’s credibility with its people and the outside world. Ultimately Russian cyber operations in Georgia assisted the Russian military in achieving its strategic goals in Georgia.
The Five Day War, according to Hollis (2011) is the first case of cyber attacks coordinated with other military operations. Reviewing the conduct of the cyber maneuvers during this war provides useful insight into future applications.

Firstly, a military objective or operating area can be isolated in cyberspace to support land operations. Such isolation can include the denial of official Internet services, disruption of cyber systems in an adversary network, and the denial of Internet communications to outside third parties. Cyber-isolation would be especially useful during decisive phases of an operation, where limiting or disrupting enemy communication’s networks domestically and internationally may contribute to achieving military objectives. A "comparative inconvenience" (isolation) was created through the disruption of banking systems, mobile telephone communications and Internet access in Georgia. Additionally, such isolation could alter and effect strategic alliances. Given the interconnected nature of cyberspace, the electronic isolation of an entire nation or even a significant portion of a nation, could create second and third order effects in other nations, bringing other unwanted players into the conflict. Alternately the same isolation could fracture an alliance before combat operations commenced, being a useful shaping action.

Secondly, narrative manipulation evident through the disruption of media communication can influence the international community’s opinion towards the conflict. Many media outlets communicate to global hubs for dissemination through systems using nodes exploitable through the Internet. The reliance on such communications systems, even satellite, is open to disruption and denial and could offer an opportunity for manipulation of the narrative regarding a conflict. Such manipulation could be swayed towards particular strategic messages that support the attainment of friendly goals. A further example of such activity is present in the conduct of cyber actions during conflict between Hezbollah and Israel from 2006. Both sides of the conflict
conducted aggressive manipulation of social media sites, public geospatial applications (such as Google Earth), and websites to influence international and domestic opinions and attitudes.27

Through exploitation of social media, online content and available media websites, manipulation of the story concerning a conflict could be undertaken (as evidenced in Georgian website defacement and on-line messaging). This could be a very powerful cyber-shaping activity, involving the full range of Information Operations and cyber capabilities to weaken or disrupt social understanding of a conflict, or alter public perceptions. Planners could then design directed messaging to local inhabitants without enemy command influence. As a trend of future conflict this element is likely to develop, given more numerous personal digital devices being connected through the Internet.28

Thirdly, cyber-blockades could contribute to the disruption of the economic infrastructure of an objective area. Such blockades could be designed akin to naval blockades, but focus on the neutralization of adversary financial conduits across cyberspace; economic trade across the Internet; and denial of services using electronic systems. While this occurred for a short period of time during the Five Day War, it could be designed by planners to last for a longer period and be used in conjunction with physical blockades of land and sea entry points. Such actions however, would require significant resources to be effective and would have many second and third order effects across the globe.

To support cyber-blockades, physical attack on Internet conduits could also be undertaken. There exists presently a number of digital ‘choke-points’ for the transfer of Internet communications through-undersea cables (appendix B provides an example), which is still the dominant medium for Internet traffic globally.29 These digital choke points could become the focus of physical attacks or disruption by a determined adversary. Efforts to physically disrupt digital choke points have been undertaken as recently as early 2013. Egyptian authorities in
March 2013 detained a number of saboteurs attempting to cut the undersea Internet cable at Alexandria connecting North Africa-Asia to Europe.30

Finally, in conjunction with cyber-reconnaissance, adversary cyber systems can be isolated to disrupt and corrupt the decision making process. Degrading or modifying information that enemy decision makers rely on can ultimately reduce the integrity of the systems and either impede operations or force the adversary to much slower forms of command and control.

Preceded by and used in conjunction with cyber-reconnaissance, cyber-isolation, synchronized with other military operations, could be a powerful tool for future military planners. Likewise, the conduct of cyber enabled strikes that cause physical damage offer some promise for future planners. This leads us to the final observation regarding future cyberspace operations.

**Strike.** According to some analysts, the Stuxnet attack during 2010 was a ‘game changer’ in the realm of cyber operations. Stuxnet was a sophisticated computer virus allegedly created by either the U.S. or Israel to attack Iranian nuclear facilities.31 Specifically, the worm, discovered in June 2010, was designed to survey and then subvert very specific industrial controls relating to Supervisory Control and Data Acquisition (SCADA) systems that monitored industrial nuclear processes. Through a precise insertion of the virus, a cyber-strike was conducted.

The aim of Stuxnet was to destroy centrifuges used in Iran’s nuclear program by disrupting the SCADA system that controls and monitors the delicate processes within uranium enrichment machines.32 Essentially, the virus was designed to cause centrifuges to spin out of control, causing damage that disrupted the enrichment of uranium. The damage to the Iranian program has been estimated at between two to four years.33 Significantly with Stuxnet, the virus was designed as malware to achieve a real-world outcome — physical destruction. This physical destruction has not before been noted in relation to a computer virus attack.34
Additionally, the virus was able to circumvent what is known as a closed network through its ability to spread via a Universal Serial Bus (USB) memory stick and other devices such as printers and scanners through the Internet. A closed network in cyberspace terms is a system not usually connected to the Internet and one that is often protected by various physical security measures, such as personnel access controls, guards, and physical barriers. Examples of closed networks include highly classified military networks and many industrial control systems. This factor is particularly relevant for military planners when considering adversary cyber systems.

The Stuxnet case study provides three learning points towards the act of cyber-strike. Firstly, a virus to be used in cyber-strike needs to be sophisticated and exact. The Stuxnet code was intricate and could selectively attack very specific industrial systems. A precise virus can only be developed through extensive cyber-reconnaissance of the target system prior to launching the attack. If a virus is not precise it could have catastrophic results. Precision viruses such as Stuxnet suggest to planners there is the ability to conduct targeted strikes against enemy facilities that may be more readily available in the future. Alternatively planners could employ focused attacks against enemy command and control nodes, or against other electronic systems that manage logistics, fuel, or operations in support of other traditional military actions.

Secondly, Stuxnet was assessed to require significant time to design and build. Lead-time in development is a significant factor to consider when using cyber weapons, specifically in relation to knowledge of adversary computer and defense systems. Such knowledge comes not only from cyber-reconnaissance but also from traditional intelligence collection and analysis.

A third lesson is that a closed network is never really ‘closed’. Stuxnet’s ability to strike against a closed network undermined a long held assumption that closed networks were generally more secure than open ones connected to the Internet. In effect Stuxnet through its design and employment was able to circumvent some of the physical security barriers put in place to protect
the targeted systems. Stuxnet’s designers exploited the fact that eventually a closed system has to be managed by humans and connected to a device (such as a USB or a laptop computer) that has most likely had contact to the Internet. Despite security procedures in place, even highly classified military systems are often exposed to such errors, and therefore open to exploitation.36 One reaction to viruses such as Stuxnet is to significantly restrict and secure the vulnerabilities they exploited, limiting future use.

Still, the U.S. military is experimenting with means to achieve the same effects of viruses such as Stuxnet, without physical connections to the closed system. The U.S. Navy is reportedly developing airborne electronic warfare systems that will be able to ‘fire’ malicious code into closed adversary networks from up to 200 miles away.37 Additionally, the U.S. Army in a similar fashion is reportedly experimenting with techniques to insert and extract data from sealed or wired networks from a standoff distance. Such technology has been termed electronic warfare enabled cyber and attempts to transmit code via radio signals into targeted computer systems.38 The potential for such weapon systems in future conflict build on that demonstrated by Stuxnet and could enable standoff disruption to enemy networks in a significant manner. In effect, Stuxnet derivative future weapons will likely negate specific modern physical defensive systems and security measures.

The final learning point observed in the Stuxnet case study focuses on the timing of cyber strike. In most cases, cyber strike weapons will likely be a ‘one-shot’ capability. Given that malicious code or viruses are developed based on vulnerabilities in the system being targeted (either virtual or physical), once the weapon is employed, the same vulnerabilities will be realized and secured, probably negating the cyber weapons’ future use. This contrasts with the employment of more traditional weapon systems that often retain their utility throughout a campaign.39 Of course, if the cyber strike is timed for specific effects ‘one-time’ may be all that is
needed. Timing in employment here is everything. Employment of weapons, such as Stuxnet or similar capabilities as evidenced in Operation ORCHARD, can be thought of as a ‘silver bullet’ capability—limited in application, but highly devastating against the right target. Employment of a war-fighting tool in this manner will require focused analysis of adversary reactions, and high levels of synchronization with other war-fighting functions.

From the brief analysis of recent case studies presented, cyber-reconnaissance, cyber-isolation and cyber-strike emerge as future shaping tools for planners. Broad considerations for the future use of the proposed cyber tools in planning follows.

CONSIDERATIONS FOR THE PLANNER IN THE USE OF FUTURE CYBER TOOLS

"Coordinated cyber attacks designed to shape the larger battle space and influence a wide range of forces and levers of power may become the key feature of the next war."

Cyber-reconnaissance. Deciding on whether to exploit the advantage gained through cyber-reconnaissance is a key consideration for military planners. Should the knowledge sourced through reconnaissance support the launching of a spectacular surprise attack, or a pre-emptive disruption of an opponent’s cyber system(s)? Or will the loss of access to the opponent’s system, due to the employment of countermeasures, be too costly to future military plans? Military planners must decide if and when to strike and be prepared to accept a potential loss in capability or access to the adversary cyber system. Such decisions should be based on strategic guidance that includes calculation of risk. Guidance that informs planners should determine whether an offensive or defensive strategy is required—each of which has different implications for cyber.

Strategic offense should rapidly gain surprise and overwhelm an adversary, but strategic defense may afford early warning through the provision of intelligence gained through analyzing what an adversary is doing to friendly systems. In general terms, the maintenance of advantage generated by cyber-reconnaissance favors the strategic defense. A defensive strategy generally provides a decision maker with the ability to discern adversary’s actions and respond
accordingly, assuming that sufficient intelligence is available. Such a strategy is particularly useful during the preliminary stages of conflict. The conduct of offensive cyber actions, encapsulated in the idea of a counterattack, within a defensive strategy should however be a key component of any strategic defensive strategy that employs cyberspace capabilities.

The use of other intelligence disciplines, maintenance of strict operational security and appropriate cyber and physical defensive systems will assist in determining when to employ cyber-reconnaissance. Determining which option to select and if a risk is worth taking based on cyber-reconnaissance effects is a basic cost benefit or intelligence loss-gain equation.

**Cyber-Isolation.** Following adequate cyber-reconnaissance, isolation of an objective by planners may also be an operational goal. The decision to conduct isolation of an objective can be made for tactical to strategic reasons. Tactically isolating an objective may involve the local disruption of Internet access or specific denial of services to cyber systems for a short period of time. Planners could ask for specific effects, such as “turning the lights off in a particular city at 0321 hours” and specialists go about designing cyber-weapons to achieve such an effect. The actions of the adversary in response to the isolation can highlight other vulnerabilities to planners to maintain watch for or to exploit.

At the strategic and operational level, isolation would likely involve the strangling of an area, state or organization for a longer period of time. Isolation could be focused on affecting the nature of a cyber system, but most likely the isolation will be part of a synchronized national power campaign, which includes other traditional war fighting functions, diplomatic activities, economic actions and particularly informational capabilities. Conflicts involving graduated escalation of force to coerce an opponent could use cyber-isolation techniques such as cyber-blockades, denial of services, and narrative manipulation.
Additionally, cyber-isolation could be effectively used to disrupt adversary alliances. Alliances can enhance the strength of a potential adversary. Alliances often create multiple fronts of conflict. Cyber-isolation employed against one ally could dissuade them from participating in a future conflict or during the preliminary stages of war, thus reducing the number of fronts. This is particularly relevant when international or regional consensus is needed to support a conflict. Similarly when a smaller adversary requires the assistance of a larger ally. Cyber-isolation could cause a fracture of an alliance by generating higher than anticipated costs to a partner through impacts on communications, economic or physical infrastructures.

Isolation of an ally combined with deception actions through cyber would also prove a useful component in future campaigns. Cyber-isolation, through employment of the means described, could achieve a level of surprise in terms of strategic attack timings and locations. In addition the conduct of deception and importantly measuring deception effects – often observed through enemy command and control reactions – would be greatly enhanced with synchronized cyber operations.

**Cyber-strike.** Cyber-strike should be employed sparingly due to the time it takes to develop a virus that is precise, guided and sophisticated. In some cases the cost of developing and employing a cyber-strike weapon may not be worth the outlay of time and resources. In other cases cyber-reconnaissance may reveal that there just aren’t the vulnerabilities to exploit using cyber previously expected by planners. Adversary counter-action capabilities and intentions must also factor into any decision to employ cyber-strike weapons.

Additionally, significant risk assessment is required to be performed prior to cyber-strike employment, not unlike that for kinetic strike operations. Risk assessment would be required to judge collateral damage, second and third order effects and likely adversary reactions. Cyber-strike can and should be employed to achieve initial offensive advantage to disrupt command
control and intelligence systems during the opening stages of an offensive, or to confuse and misdirect opponent's reactions as part of a deception plan. An adversary's critical infrastructure could also be targeted using cyber-strike to disrupt essential services to civilians and deny supporting assets to militaries, in conjunction with other military actions. A graphical summary of all three cyber-shaping tools and key considerations for planners is provided in appendix C.

The employment of the three cyber-shaping tools in a military operation will provide an edge over potential adversaries. For the effects to be advantageous, planners and cyber-specialists, both those designing and crafting the cyber weapons and their managers, need to be in constant dialogue. This dialogue is vital to achieve a shared understanding of the problem and likely solutions, best achieved through the presence of cyber-specialists within planning teams and deployed headquarters. Guided by this shared understanding, cyber specialists can then best support planners. Planners will then be in a position to leverage the most from what cyberspace can offer the war-fighter.

CONCLUSION

As military forces across the globe wrestle with the impact of cyberspace and a vastly more digitally interconnected battle space, planners of the future will require a sound understanding of cyberspace and what it can offer commanders to enable military success. Success for planners at the operational level will involve the articulation and execution of operations and campaigns that achieve the goals and political objectives set for them. Current and future developments in cyberspace offer planners a number of tools to assist in the crafting of successful designs through shaping of the battle space.

The cyber shaping tools articulated within this paper provide a broad approach to maximizing the unique characteristics of cyberspace. As future adversaries continue to explore more technical and digitally connected means of conducting and enabling war fighting the
demonstrated characteristics of cyberspace operations will provide military planners, based on projected development trends, with unique battle space shaping tools, including cyber reconnaissance, isolation and strike that can greatly enhance the future conduct of war fighting.

1 Michael V. Hayden, "The Future of Things “Cyber”," (Strategic Studies Quarterly, Volume 5, Number 1, Spring 2011), 3.
5 A recent example of such a non-state group is the Islamic hacker group Izz ad-Din al-Qassam Cyber Fighters, who have claimed responsibility for a number of DDOS attacks against U.S. banks during late 2012 and early 2013, under ‘Operation Ababil’, in response to the YouTube Muhammad movie released online in 2012.
7 James R. Clapper, “Worldwide Threat Assessment of the US Intelligence Community,” Statement for the Record to Senate Select Committee on Intelligence (March 12, 2013), 1.
8 US Cyber Command was established at Full Operating Capability in October 2010.
10 One reason for a lack of clarity on this line of discussion is the pace of development of threats and countermeasures in cyberspace, coupled with the highly classified and sensitive nature of offensive cyberspace capabilities. Authors own assessment based on interviews with US CYBERCOMD personnel, November 2012.
11 United States Government Accountability Office, 5
12 Reconnaissance is defined as “A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.” United States Department of Defense, Joint Publication 1-02 Dictionary of Military and Associated Terms (Washington, DC: U.S. Department of Defense, May 15, 2011), 305.


A brief but useful overview regarding the background and employment of ULTRA and other Allied signals intelligence during WWII is provided in Jeffrey T. Richelson, A Century of Spies – Intelligence in the Twentieth Century (Oxford, UK: Oxford University Press, 1995), 173-197.


By 2030, Internet trends will likely include: terabit internet speed as standard; 5G-7G cell phone networks; over 8 billion people in the global online community; the majority of ‘things’ connected permanently to the internet; and available internet globally.


Paulo Shakarian, “The 2008 Russian Cyber Campaign Against Georgia” (Military Review, November-December 2011), 64.


Hasan M. Al-Rizzo, “The Undeclared Cyberspace War Between Hezbollah and Israel” (Contemporary Arab Affairs, Vol 1, No. 3, July 2008), 400.


In March 2013, individuals were arrested by Egyptian authorizes attempting to cut the undersea Internet cable system located near Alexandria. The cable – SEA-ME-WE4 – is a key conduit for traffic from Asia and Europe. While there is some redundancy in undersea cables, even one disruption can significantly slow or impede Internet traffic. Synchronized with electronic cyber isolation techniques such as DDOS, this could be an effective means to target an objective.

Leo Mirani, “Forget about the CyberBunker attack – here’s how to take an entire continent offline,” (Quartz Online, March 28, 2013). http://qz.com/68115/forget-about-the-cyberbunker-attack-heres-how-to-

31 The Stuxnet attack was reportedly known as Operation OLYMPIC GAMES. David E. Sanger, Confront and Conceal – Obama’s Secret Wars and Surprising Use of American Power (New York, NY: Random House, 2012), 188.

32 Shawn Collins and Stephen McCombie, “Stuxnet: the Emergence of a New Cyber Weapon and its Implications”, (Journal of Policing, Intelligence and Counter Terrorism, Vol 7, No 1, April 2012), 84.

33 Ibid, 86

34 Ibid, 87

35 Ibid, 86


39 Libicki, 331

BIBLIOGRAPHY

Books


Military Doctrine


**US Government Policy – Documents**


**Reports**


Academic Papers


Journal Articles


**Websites and Blogs**


**News Articles**


Appendix A - Cyber-Attack Cycle

Figure 1. Cyber-Attack Cycle. Note: This cycle is similar in concept to intelligence collection cycle used by many intelligence agencies. Source: Mandiant, “APT 1 – Exposing One of China’s Cyber Espionage Units” (February 2013), 27 http://www.mandiant.com/ (accessed: February 20, 2013)
Appendix B - 2012 Submarine Fiber Optic Cable Map

Figure 2. 2012 Submarine Fiber Optic Cable Map. Annotated map highlights some examples of possible digital physical chokepoints. Source: http://www.telegeography.com/telecom-resources/map-gallery/submarine-cable-map-2011/index.html (accessed: March 1, 2013)
Appendix C - Planners Considerations for Offensive Cyber Tools Employment

Figure 3. Suggested considerations for planners employing offensive cyber tools.

Source: authors own graphic.