AIR WAR COLLEGE

AIR UNIVERSITY

CYBER: A FLEXIBLE DETERRENT OPTION

By

Harold T. Hoang, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. George Stein

14 February 2013

DISTRIBUTION A. Approved for public release: distribution unlimited

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Abstract

The recognition of cyberspace as the fifth domain for warfare introduces similar challenges that early warfighters and planners faced, planning and executing military operations in the land, sea, air, and space domains. Though it is considered a man-made domain, the cyber domain is more complex with no established norm of behaviors and without borders. If history is a teacher then the United States military will find ways to gain cyber superiority, although critics would argue that there is no such thing as cyber superiority. Additionally the US military continues to struggle with its thinking and approach as to how to wield cyber power in and through what is now considered a contested domain. Some of the issues facing commanders and cyber operators include obtaining legal authority to pursue an adversary across sovereign "borders", division of labor among statutory titles, agencies and departments within the US government, balancing intelligence gain and loss, and the difficulty of attribution. The first step to overcoming the operational challenges is to recognize that planning and executing cyber operations should not be any different than planning and executing operations in the air, land, and maritime domains.

While deterrence has always been part of the US military strategy cyber as a flexible deterrent option is not currently in the tool kit for the Joint Forces Commanders to draw from. Although USSTRATCOM may have the expertise and experience regarding deterrence, 24th Air Force should pursue and develop a cyber force competent in the art of cyber deterrence and be the lead to create a cyber operational plan to ensure full spectrum cyber operations in support of the JFCs. More importantly 24 AF should adopt and apply the Single Integrated Operational Plan, the United States' general plan for nuclear war from 1961 to 2003, and the Joint Operation Planning Process as the model to use in planning and employing cyber power in support of JFCs.

Digital Collections

Biography

Lieutenant Colonel Hoang entered the Air Force in 1991 as a Distinguished Graduate from the Reserve Officer Training Corps at the Oregon State University, Oregon. His career highlights include service a deputy mission support group commander and the Commander, Communications Support Squadron. He has served as a flight commander, information operations planner, ROTC instructor, Assistant to Air Force Space Command Director of Staff, and executive officer to Air Force Space Command Vice Commander. Colonel Hoang has deployed in support of Operation ENDURING FREEDOM and Operation SOUTHERN WATCH. He served one year at Headquarters United States Forces Korea responsible for planning and executing the non-combatant evacuation operations. Colonel Hoang wears the master cyberspace operator badge.

Digital Collections
Air University–Maxwell AFB, AL

Introduction

> *"We are at a nexus regarding future cyberspace operations providing for the National Defense. In order for the Air Force to fulfill our commitment to provide Global Vigilance, Reach, and Power, we must do what Airmen have always done -- innovate."*[1]
>
> *Major General Suzanne M. Vautrinot*

The recognition of cyberspace as a fifth domain of warfare presents military commanders and practitioners with the challenges of integrating cyber capabilities into a coherent extended deterrence strategy in and through the cyberspace domain. More importantly cyber capabilities are not yet fully developed to offer commanders flexible deterrent options to deter conflict.

I echo Major General Vautrinot's sentiment that as Airmen we believe that things could always be better; there is a better way to get the mission done. That kind of thinking or paradigm is in our DNA. To illustrate this point the thesis of my paper is to adopt and apply the Single Integrated Operational Plan (SIOP), the United States' general plan for nuclear war from 1961 to 2003, and the Joint Operation Planning Process (JOPP) as the model to use in planning and employing cyber power in support of Joint Forces Commanders (JFCs). The dual role of the SIOP, deterrence and warfighting should deterrence fail, is a model that is adaptable to the use of cyber power: pre-, during, and post-conflict. More specifically 24th Air Force (24 AF) can apply this concept in planning and presenting cyber forces and capabilities through the US Cyber Command (USCYBERCOM) in support of combatant commanders during the road to conflict. By adapting cyber power as a deterrent capability through an effective Intelligence, Surveillance, and Reconnaissance (ISR) effort, and expanding operational concepts, the AF will offer commanders a flexible deterrent option (FDO) to meet fast-moving challenges of an adversary seeking "to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD's information

infrastructure."[2] In other words, when directed, the 24 AF will be able to deliver cyber capabilities in support of the JFCs requirements to deter or counter the threat.

To set the stage I will revisit the classical deterrence strategy as a proven model with the goal of identifying possible tactics, techniques and procedures (TTPs) that may be readily transferable and adaptable to the cyber domain. More importantly I will examine and analyze the rigor and discipline behind the planning process that would be suitable and relevant for the purpose of this paper. Next I will address the limiting factors (LIMFACs) such as attribution and intelligence gain and loss merely to acknowledge their existence and to make readers aware of such LIMFACs. Finding solutions to overcome these LIMFACs, however, is beyond the scope of this paper. Instead through the use of the SIOP model and the JOPP I will propose a solution by taking an operational planning approach to present cyber capabilities as a flexible deterrent option to commanders prior to conflict escalation, thereby, overcoming the LIMFACs. Based on the SIOP model, I will examine some possible scenarios, targets and outcomes where cyber capability is used to deter with the intent of deescalating the conflict. I will conclude by summarizing the benefits of applying the SIOP rigor and using the JOPP to the cyber domain along with making recommendation for 24 AF considerations as the AF continues to improve its application of cyber capabilities.

Classical Nuclear Deterrent Model

Deterrence has always been part of the US military strategy. The classic means of deterrence has been a demonstration of force through exercises that may involve massing of military personnel, equipment, air shows, and with the nuclear arsenal as the backstop should deterrence fail. In his book, *The Bomb,* Stephen M. Younger suggests that, "Deterrence served as a form of nuclear defense during the Cold War—no one wanted to risk the threat of massive

retaliation by initiating a nuclear attack."[3] Younger's assertion implies that deterrence is effective when dealing with rational state-actors, during the Cold War the rational actors were the United States and the Soviet Union. James Schlesinger, former secretary of defense, reasoned "that the extreme damage caused by a counterattack essentially self-deterred the United States from ever using nuclear weapon"[4] further supports Younger's assertion. On the contrary the 2010 US National Security Strategy identifies that "the American people face no greater or more urgent danger than a terrorist attack with a nuclear weapon"[5] highlights a different concern when dealing with irrational actor such as terrorist. In other words, deterrence may not be an effective mean to use against irrational actors. It is important then for cyber planners and operators to keep these assertions in mind as they move forward with employing cyber power.

Another point of contention has to do with the question of whether or not the US nuclear deterrent posture was key to the United States winning the Cold War. Some would consider that Younger further fuels the debate by saying, "The end of the Cold War was unusual in that it was less of a victory by the West than it was a self-generated collapse by the East."[6] Similarly the same debate could be applied to how World War II in the Pacific ended. Many in the United States would say that the dropping of two atomic bombs on the cities of Hiroshima and Nagasaki caused the Japanese to surrender while the Soviet Union would say that Japan surrendered because of the eminent threat from the Soviet Union entering the war. Yet Japan would counter with its own version—Japan was ready to consider a cease-fire to end the war without the need for the atomic attacks. Regardless of the debate, the main take away is that there were key nuclear war planning tenants that could be adapted to the cyberspace domain.

Digital Collections

Single Integrated Operational Plan

During the Cold War US military planners developed the SIOP to present the US President with quick nuclear response options in the event of a nuclear attack against the US homeland.[7] The SIOP gave the US President a range of targeting options to include launch procedures and which nuclear warheads would be launched against predetermined target sets.

The specific details regarding types of nuclear warheads to be used, target selection, target application of the United States' nuclear war planning process remains classified. However the unclassified portion of the SIOP planning process provides an overview of the process that starts when the US President issues a directive outlining the concepts, goal, and guidance to the nuclear planners. The Secretary of Defense (SecDef) takes the President's directive to develop the Nuclear Weapons Employment Policy (NUWEP) that includes assumptions and other planning factors such as attack plans, objectives, target selections, and constraints. The Joint Chiefs of Staff (JCS) uses the NUWEP to provide detailed instructions to the US Strategic Command (USSTRATCOM) for the final phase of the planning process. Based on SecDef's guidance USSTRATCOM creates the nuclear war plan that becomes the SIOP. According to the Natural Resources Defense Council, "The SIOP is not one plan or one option, but a set of plans and a series of options constructed from a single target set contained in the NTB."[8]

As briefly described above the SIOP planning process starts at the direction of the US President and progresses through series of stages that could take up to 18 months to develop. The Natural Resources Defense Council identified the major SIOP planning steps as:

> a. **Target development:** The National Strategic Target List (NSTL) will consist of those target installation the destruction or neutralization of which will accomplish the essential national task.
> b. **Desired Ground Zero (DGZ) Construction:** Grouping installations into

aimpoints for weapon allocation, and compiling the coded aimpoints into the National DGZ List (NDL). DGZs are characterized in terms of time sensitivity, location, hardness, priority, defenses, and damage requirements.

c. **Assignment:** Includes the following steps:

1. *Weapon Allocation:* Assignment of ICBM and SLBM warheads in an initial strike, and aircraft bombs and cruise missiles in a generated-alert strike or follow-on strike to specific aimpoints
2. *Weapon Application:* Allocation and assignment of specific warheads on specific delivery systems to the DGZ, including setting timing, development of aircraft routes, consideration of defenses, etc.
3. *Timing and Deconfliction:* The choreography of the attacks is analyzed to insure there are no conflicts among warhead detonations and flight plans

d. **Reconnaissance Planning:** Dedicate necessary national assets for intelligence gathering against targets identified in the NSTL.

e. **Analysis:**

1. *War Gaming*
2. *Consequences of Execution (C of E) Analysis:* Damage assessments, including physical damage, fatalities, population at risk from prompt and delayed nuclear effects, force attrition, and the degree the plan meets guidance

f. **Document Production**[9]

As I will demonstrate later in the paper these major steps are very applicable to the cyber domain and should be used as a model for planning and employing cyber power.

Cyber Offensive Operation Challenges

Operating in and through the cyber domain has its challenges. Some of the issues facing commanders and cyber operators include obtaining legal authority to pursue an adversary across sovereign "borders", division of labor among statutory titles, agencies and departments within the US government, balancing intelligence gain and loss, and the difficulty of attribution. In his testimony at his confirmation hearings before the Senate, Lieutenant General Keith Alexander explained, "There is no international consensus on a precise definition of a use of force, in or out of cyberspace."[10] These challenges seem insurmountable, when taking at face value, with prescribed artificial constraints putting cyber operators into a virtual box. However addressing these challenges or limiting factors (LIMFACs) from a different perspective, both in time and

space, allows cyber operators the freedom of actions to develop solutions that were not there before. I offer a perspective that rejects the view that the "attribution problem" wholly paralyzes any attempt to develop effective cyber flexible deterrent options in support of the JFCs.

Cyber deterrence is currently not in the military lexicon. Active cyber deterrence, similar to nuclear deterrence, when synchronized with other military capabilities demonstrates a military resolve to deter rational adversaries from causing harm to our networks, to prevent potential unintended escalation of warfare in cyberspace that could globally consume all nations, in essence realizing a "mutually assured destruction" scenario. However unlike nuclear deterrence, demonstrating cyber deterrence could compromise intelligence gathering capability, sacrificing the long-term intelligence gain from an exploited source. More importantly cyber operators must synchronize and deconflict cyber operations across other security and intelligence agencies to minimize fratricide in cyberspace.

The 21st Century military considers cyberspace as a new warfare domain that can be exploited across multiple disciplines coexisting on the same network; banking, commerce, social, industrial, and in warfare. Globalization further emphasizes this symbiotic relationship across geographic borders among governments and businesses. This is could be seen as a positive dependency as Dr. Kamal T. Jabbour, ST, Senior Scientist Information Assurance at the AF Research Laboratory, pointed out, "Assured mutual co-existence provides some form of deterrence in the cyberspace domain of today."[11]

The US military strategic thought has always been oriented toward dominance in space, air, land, sea, and now cyberspace to ensure our freedom of actions while denying the same to adversaries. Although the US military has no equal at dominating the air, land and maritime domains during conflicts, pursuing cyber dominance would not be as easy or even possible given

the fact that most of the cyberspace domain is "often privately owned, and primarily civilian in use"[12] that spans the whole globe. Perhaps gaining a relative advantage in a contested and ever changing domain may be sufficient to get the mission done. Recognizing this challenge, the US Cyber Command Operational Directive 12-001 assigns roles and responsibilities to AFCYBER to identify requirements for, and advocate for development of, cyber capabilities and TTPs for specific target sets.[13] Similarly the Air Force Cyber Vision 2025 (CV2025) emphasizes assured cyber advantage across air, space, cyberspace, C2, ISR and mission support.[14] However CV2025 asserts that the Air Force will leverage USSTRATCOM expertise in cyber strategy and deterrence. While USSTRATCOM may have the expertise and experience regarding deterrence, 24 AF should pursue and develop a cyber force competent in the art of cyber deterrence and be the lead to create a cyber operational plan to ensure full spectrum cyber operations in support of the JFCs.

Joint Publication 5-0, *Joint Operation Planning,* identifies six distinct planning phases in support of a military operation. The phases most applicable to the deterrent theory are Phases 0 and 1. During Phase 0, operations in the cyber domain as well as operations in the other domains are designed "to dissuade or deter potential adversaries."[15] Likewise the notional intent of Phase 1 "is to deter undesirable adversary action by demonstrating the capabilities and resolve of the joint force."[16] More importantly, Phase 1 activities leverage "on security cooperation activities from phase 0 and are conducted as part of security cooperation activities."[17]

Cyber power could be one of the many capabilities or flexible deterrent options available to the JFCs to dissuade or deter an adversary before a full-scale conflict erupts. Flexible deterrent options "assist in bringing an issue to early resolution before armed conflict by sending an appropriate message to belligerent parties."[18] Furthermore FDOs enable "an early decision by

laying out a wide range of interrelated response paths that are carefully tailored"[19] to mitigate commander's concerns of not responding proportionately to a threat. As defined by Joint Publication 5-0:

> Flexible deterrent options (FDOs) are preplanned, deterrence-oriented actions carefully tailored to send the right signal and influence an adversary's actions. They can be established to dissuade actions before a crisis arises or to deter further aggression during a crisis. The FDOs are developed for each instrument of national power—diplomatic, informational, military, and economic--but they are most effective when used to combine the influence across instruments of national power. Additionally FDOs facilitate early strategic decision-making, rapid de-escalation, and crisis resolution by laying out a wide range of interrelated response paths.[20]

Joint Publication 5-0 also identifies the key goals of FDOs as:

> a. Deter aggression through communicating the strength of US commitments to treaty obligations and regional peace and stability.
> b. Confront the adversary with unacceptable costs for their possible aggression.
> c. Isolate the adversary from regional neighbors and to split the adversary coalition.
> d. Rapidly improve the military balance of power in the area of operations without precipitating armed response from the adversary.[21]

For cyber operations, once an adversary initiates a crisis the LIMFACs, mainly the attribution issue, is no longer a constraint. As the United States prepares to apply its national instruments of power to prevent a crisis from escalating, cyber power could be fully employed as part of the overall national effort to dissuade and deter an adversary.

Applying the SIOP Model to Cyber

Adopting the SIOP model is the first step toward delivering credible cyber capabilities to the JFCs. Additionally cyber planners should follow the JOPP "orderly, analytical process, which consists of a set of logical steps to examine a mission; develop, analyze, and compare alternative COAs; select the best COA; and produce a plan or order"[22] to synchronize cyber capabilities into a master attack plan. JOPP is a proven method to capture commanders' intent

while synchronizing staff's work in developing plans that will sufficiently meet mission requirements.

Using the nuclear SIOP as the model and the JOPP as a guideline, cyber operators could develop an integrated cyber operational plan that identifies potential target sets; matching specialized cyber capabilities against those target sets as well as develop generalized cyber capabilities that would be applicable against any adversary. The cyber integrated operational plan would be applicable during the Phases 0 and 1 of operation as flexible deterrent options; however, the plan is applicable throughout the conflict spectrum.

Combatant Commanders are accepting cyber as an element of combat power rather than viewing it as merely a support function for operations in the other domains. In a recent Operations Directive, the Commander, USCYBERCOM directed that each Service Component engage and conduct mission analysis with an emphasis that, "Cyber capabilities are driving a change in the way we plan, and they require both flexibility and a focused, detailed understanding of the cyber environment."[23] If cyberspace is a "man-made domain"[24] it should not be so mysterious that would prevent the US military from operating "effectively in all domains- air, land, maritime, space, and cyberspace."[25]

Major General Brett Williams, US CYBERCOM Director of Operations, suggested that "At the operational level of war, operations in cyber should be planned and executed in the same manner as operations planned and executed in the air, land and maritime domains."[26] In a speech at the Intrepid Sea, Air and Space Museum in New York, Defense Secretary Leon E. Panetta warned "that the United States was facing the possibility of a "cyber-Pearl Harbor" and was increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government."[27] This is not a new revelation

but merely recognition of today's electronically interconnected and contested environment the United States shares with its allies and adversaries. The speed at which activities happen in cyberspace further complicate the problem and in some cases demands a decision and actions in seconds rather than minutes or hours. Cyber operators must have an approved synchronized plan ready for execution to have any hope of taking advantage of fleeting opportunities in cyberspace.

Key elements to mission planning include national and military strategic guidance and the commander's intent. Joint Publication 5-0 stresses that "it is essential that the tasks (specified and implied) and their purposes are clearly stated to ensure planning encompasses all requirements; limitations (restraints--cannot do, or constraints--must do) on actions that the commander or subordinate forces may take are understood; and the correlation between the commander's mission and intent and those of higher and other commanders is understood."[28]

a. **Target development:** While the National Strategic Target List is an installation-centric, cyber planners can adopt the same targeting concept to develop a target set more conducive to cyber operations. Using the targeting framework and targeting cycle as outlined in Joint Publication 3-60, *Joint Targeting,* cyber operators will be able to synchronize cyber effects with other joint fires while minimizing unintended collateral effects. Joint Publication 3-60 identifies targeting principles as:

> 1. The targeting process is focused on achieving the JFC's objectives.
> 2. Targeting is concerned with the creation of specific desired effects through target engagement.[29]

Based on the desired effect to be achieved the SIOP planners used the " countervalue and counterforce"[30], analogous to the Center of Gravity concept, approaches to determine nuclear targeting. To the planners "countervalue targeting aims to destroy cities, populations, and other things of value to shock the enemy into ceasing hostilities"[31] – to break the adversary's will to

wage war. On the other hand, counterforce targeting main objective is to destroy adversary's "military bases, missile fields, submarines, and other targets of strategic value"[32] reducing his capability to conduct hostility or continued to cause more damage.

While cyber power is capable of striking countervalue and counterforce targets, or set the conditions for other joint fires to achieve the desired effects, the type of targets to attack will depend on the JFCs intent. Based on recent US military operations an adversary could expect that the JFCs will seek to achieve air superiority and taking out its command and control capability to gain an operational advantage. The adversary would expect that kinetic means would be the weapon of choice to destroy these target sets. But if cyber experts were correct in predicting that future wars will start in cyberspace, it would be prudent for the US military to expect that the adversary will use cyber as asymmetric means to initiate conflict against the United States. What countervalue and counterforce targets in the United States will the adversary go after? It would be safe to surmise that the adversary paid attention to what Secretary of Defense Panetta said about the United States vulnerabilities in cyberspace. Logic would dictate that an adversary would take precautionary measures to harden their critical infrastructure to minimize vulnerabilities. Following the same line of thought, exploiting an adversary's "power grid, transportation system, financial networks and government"[33] vulnerabilities through cyber means would be a good starting point for the US military in an effort to dissuade and deter an adversary from initiating conflict.

Employing cyber power in a notional scenario to achieve a deterrent effect could be played out as follows. Keeping in mind that these targets could be degraded in a simultaneously choreographed attack or on an escalating scale based on desired effect and the adversary's reaction.

1. Power Grid: The American people expect the light to come on when they throw a switch and other electrical appliances throughout the house to work without any commercial power interruption. For power plants this means maintaining the electrical grid and the supervisory control and data acquisition (SCADA) systems at a reliable rate of "99.99999 percent of the time."[34] The standard may not be the same for an adversary but having a reliable power grid to maintain command and control during peacetime would be just as important for an adversary, even more critical during a crisis. In early 2007, researchers at the Idaho National Laboratory demonstrated a cyber capability that destroyed one of the generators from the Alaska grid. Researchers dubbed the project AURORA[35] where they took a generator from Alaska "carefully reconnected elsewhere and they blew the turbines apart by hacking into the digital devices that regulated power on the grid."[36] The researchers "simply instructed it to make rapid changes in the electricity cycles that powered the equipment: fast, slow, fast, slow. Then they just waited a second or two for the big diesel-electric generator to explode"[37] The once isolated SCADA network, in the hope of protecting it from unauthorized cyber intrusions, is no longer the case with a growing trend toward networking such systems. Recent study in "fourteen countries showed that three fourths of such systems were connected to the Internet or some other IP network."[38] Crippling any portion of a power grid would cause, at minimum, a regional blackout that could convince an adversary to think twice before proceeding with his plan to start a conflict with the United States.

2. Military communications, command and control, intelligence (C3I): The Chinese recognized that control of information was "the new strategic high ground and the linchpin of the modern American way of war."[39] This assertion is not far from the truth as the United States has demonstrated its ability to destroy an adversary's "high ground" during the

Persian Gulf War and every conflict since, while enjoying near-real time C3I throughout the operational environment. However, having a good C3I is certainly a strength to any military it could also be a vulnerability. Rendering a government and military "blind and deaf"[40] by disrupting, degrading or corrupting its information systems would not only impede its war making capability but perhaps would also change his motive to initiate hostility.

3. Enemy Integrated Air Defense System (IADS): The enemy IADS is susceptible to a cyber attack due to its connectivity and reliant on other information systems to provide targeting coordinates and attacks profiles. First, through cyber means the enemy IADS could be disabled before and during US air strikes making the system useless. Second, the system could be fooled to engage targets that are not there or looking for targets in the wrong sector, again rendering it useless. Finally, if the adversary is trying to hide their IADS to prevent its destruction, employing a "wake up" command would allow US military planes to track and destroy the IADS at will making it safer for US planes to gain air superiority.

b. **Desired Ground Zero (DGZ) Construction:** DGZs are characterized in terms of time sensitivity, location, hardness, priority, defenses, and damage requirements. The same thought process could be directly applied to delivering effect through cyber means.

c. **Assignment:** Includes the following steps:

1. *Weapon Allocation:* Depending the desired effect and the accessibility of the intended target cyber operators will assign the appropriate cyber weapon to achieve the mission. Matching effects, through the use of cyber power, against established target sets should be accomplished within the joint targeting coordination boards (JTCB). The JTCB has the responsibility to conduct planning, coordination, and deconfliction associated with joint targeting. As an example, employing a denial of service attack maybe sufficient to degrade a

military network while conducting zero-day attack against a DGZ target could deter an adversary from further aggression.

2. *Weapon Application:* Cyber planning requires significant lead time to work through the coordination and approval process for timing, development of cyber paths, consideration of cyber defenses, and weapon application. As an example, the use of Stuxnet to degrade Iran's nuclear enrichment program highlights the effort and time require from the planning for the attack to the execution Stuxnet.

Some experts considered Stuxnet as "a relatively unsophisticated Frankenstein patchwork of existing tradecraft, code and best practices drawn from the global cyber-crime community."[41] However Lieutenant Colonel Andrew C. Foltz emphasizes that Stuxnet "true sophistication lies in the synergy of its components and its method of infection."[42] He further described its sophistication by stepping through how Stuxnet worked.

> First, Stuxnet's designers required incredibly precise intelligence about Iran's PLCs and frequency converters, as well as the performance parameters of Iran's centrifuges. Second, the malware was self-replicating and designed to infect systems that were not connected to the Internet ("air-gapped"), thereby requiring the use of intermediary devices such as thumb drives. Stuxnet also employed four "zero-day" exploits and two stolen digital signatures to gain access to targeted systems. Finally, Stuxnet appears to have been designed to avoid collateral damage. If the malware did not detect the specific software-hardware configuration associated with Iran's enrichment program, the program would lie dormant. It was also designed to delete itself from thumb drives after infecting three machines, and it contained a built-in self-destruct feature. Thus, even though the worm is reported to have infected more than 100,000 hosts in 155 countries, 60% of the infections were localized to Iran, and there are no reports of physical damage outside of Iran.

3. *Timing and Deconfliction:* The choreography of the attacks is analyzed to ensure there are no conflicts among cyber "flight plans" and target manipulations while other efforts may be taking place against the same target. The key to effective integration of joint fire support is the thorough and continuous inclusion of all component fire support elements in the

joint planning process, aggressive coordination efforts, and a vigorous execution of the plan.

d. **Reconnaissance Planning:** Preparation of the cyber battle space requires significant Intelligence, Surveillance, and Reconnaissance (ISR) support. Cyber operators should leverage the expertise and capability from the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) and its counterparts to achieve full spectrum cyber operations. The AFDD 3-12, *Cyber Operations,* tasked AFISRA "To enable 24 AF operations, AFISRA provides all-source cyber-focused ISR including digital network analysis to 24 AF through the 659th ISR Group."[43] It also identified AFISRA support to be "within five cyber-focused ISR areas: current intelligence and reporting, indications and warning, threat attribution and characterization, JIPOE, and computer network exploitation."[44] Maintaining the cyber situational awareness is key to affording the JFCs the relative advantage over an adversary.

Furthermore operations in cyberspace have significantly compressed decision cycle require predetermined rules and prioritized feed for ISR actions. The 659th ISR Group has existing capabilities that are readily transferable to identifying and developing target sets, based on the JFCs predetermined COG priorities, to create the desired effects in support of the JFCs.

e. **Analysis:**

1. *War Gaming:* Cyber attack plan, synchronized with other joint fires, has to be fully played out to demonstrate its capability but more importantly to determine if the plan will achieve its desired effect. Exercise simulation may have worked well in the past but should not be the norm for today's environment. Commanders should be able to fight through a cyber attack in cyber battle labs to recognize the full affect of a cyber attack.

2. *Consequences of Execution (C of E) Analysis:* Cyber battle damage assessments must be accomplished to determine whether a "restrike" is necessary to achieve the

desired effect. Realistic measure of effectiveness must be established as a feedback mechanism to leverage other joint fire capabilities as needed.

f. **Document Production:** Codifying the tactics, techniques, and procedures (TTPs) is crucial for enduring success. As an example, the 92nd Information Operations Squadron led the creation of the "first team and the tactics employed to identify, pursue, and mitigate threats impacting critical links and nodes."[45] Its tactics were demonstrated at the first Cyber Flag exercise. The key to its mission success "was identifying and focusing on a Combatant Command's prioritized "defended asset list," those critical areas that must be able to operate through an attack."[46] Their TTPs were documented and shared as best practices, now part of the training curriculum of future cyber operators, and "may represent one of the most viable missions for expansion."[47]

Conclusion

The Air Force has made great advances in realizing the full potential of employing cyber power and will continue to do so to deliver cyber capabilities in support of the JFCs. The 24 AF should adopt a proven framework and key tenants of the SIOP model and the JOPP to plan cyber operations to maximize its contribution to the joint fight. Cyber operators should use similar rigors used to plan a nuclear war to formulate a well thought-out, synchronized and de-conflicted cyber operation plan in support of JFCs intent. Because of the speed at which the cyber environment changes it is even more critical to have an approved cyber plan ready for execution to gain a relative advantage of fleeting opportunities against an adversary to dissuade and deter aggression. As the Air Force cyber component to USCYBERCOM, 24 AF should lead Airmen's effort to expand cyberspace capabilities, more importantly helps Airmen and Joint warfighters understand cyberspace operations.

Muir S. Fairchild Research Information Center
Digital Collections
Air University Maxwell AFB, AL

Notes

1 Maj Gen Suzanne M. Vautrinot, Department of The Air Force Presentation to The Subcommittee On Emerging Threats and Capabilities House Armed Services Committee and U.S. House of Representatives, *Improving Military Capabilities For Cyber Operations*, July 25, 2012, 3.

2 Department of Defense, *Strategy For Operating In Cyberspace*, July 2011, 1.

3 Stephen M. Younger, *The Bomb A New History*, HarperCollins Publishers, New york, NY 10022, 2010, 156.

4 Ibid.

5 *The United States National Security Strategy*, May 2010, 31.

6 Stephen M. Younger, *The Bomb A New History*, HarperCollins Publishers, New york, NY 10022, 2010, 7.

7 Ibid., 52.

8 Natural Resources Defense Council, *The U.S. Nuclear War Plan: A Time For Change*, June 2001, 9.

9 Ibid, 10.

10 LTG Keith Alexander, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, US Cyber Command," Senate Armed Services Committee, 14 Apr 10.

11 Dr. Kamal T. Jabbour, ST Senior Scientist Information Assurance, AF Research Laboratory, *50 Cyber Questions Every Airman Can Answer*, May 2008, 10.

12 Department of Defense, *Strategy For Operating In Cyberspace*, July 2011, 5.

13 U.S. Cyber Command Operational Directive 12-001, April 2012.

14 Dr. Mark T. Maybury, AF Chief Scientist, *Air Force Cyber Vision 2025*, July 2012.

15 Joint Publication 5-0, *Joint Operation Planning*, 11 August 2011.

16 Ibid.

17 Ibid., III-42.

18 Ibid., E-2.

19 Ibid.

20 Ibid., E-1.

21 Ibid.

22 Ibid., XXV.

23 U.S. Cyber Command Operational Directive 12-001, April 2012.

24 Department of Defense, *Strategy For Operating In Cyberspace*, July 2011, 5.

25 Ibid.

26 Maj Gen Brett T. Williams, *"Ten Characteristics of Cyberspace Conflict,"* 6 February 2013.

27 The New York Times, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, 11 Oct 2012.

28 Joint Publication 5-0, *Joint Operation Planning*, 11 August 2011.

29 Joint Publication 3-60, Joint Targeting, 13 April 2007.

30 Stephen M. Younger, *The Bomb A New History*, HarperCollins Publishers, New york, NY 10022, 2010, 100.

31 Ibid.

32 Ibid.

33 The New York Times, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, 11 Oct 2012.

34 Joseph Weiss, *Protecting Industrial Control System from Electronic Threats,* New York Momentum Press, 2010, 8.

35 Steve Kroft, *"Cyber War: Sabotaging the System, 60 Minutes"*, July 13, 2010. http://www.cbsnews.com/video/watch/?%20id=6578069n&tag=related

36 Joel Brenner, *America The Vulnerable, Inside The New Threat Matrix Of Digital Espionage, Crime, and Warfare*, The Penguin Press, New York, 2011, 92.

37 Ibid., 93.

38 Stuart Baker, "*In the Crossfire: Critical Infrastructure in the Age of Cyber War,"* Center For Strategic and International Studies and McAfee, January 28, 2010, 19.

39 Joel Brenner, *America The Vulnerable, Inside The New Threat Matrix Of Digital Espionage, Crime, and Warfare*, The Penguin Press, New York, 2011, 120.

40 Ibid., 122.

41 Andrew C. Foltz, Stuxnet, "Schmitt Analysis," and the Cyber "Use of Force" Debate, *Joint Forces Quarterly*, Issue 67, 4th Quarter 2012, 44.

42 Ibid.

43 Air Force Doctrine Document 3-12, *Cyberspace Operations*, 15 July 2010, 24.

44 Ibid.

45 Maj Gen Suzanne M. Vautrinot, Department of The Air Force Presentation to The Subcommittee On Emerging Threats and Capabilities House Armed Services Committee and U.S. House of Representatives, *Improving Military Capabilities For Cyber Operations*, July 25, 2012, 6.

46 Ibid.

47 Ibid.

Fairchild Research Information Center
Air University–Maxwell AFB, AL

Bibliography

Air Force Doctrine Document 1-1, *Leadership and Force Development*, 8 November 2011.

Air Force Doctrine Document 3-12, *Cyberspace Operations*, 15 July 2010.

Assistant Secretary of Defense, *Guidance for Preparation of Single Integrated Operational Plan – 1963 (SIOP-63)*, 28 August 1997.

Baker, Stuart, "*In the Crossfire: Critical Infrastructure in the Age of Cyber War,"* Center For Strategic and International Studies and McAfee, January 28, 2010.

Brenner, Joel, *America The Vulnerable, Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, The Penguin Press, New York, 2011.

Boot, Max. *War Made New: Technology, Warfare, and the Course of History, 1500 to Today.* New York: Gotham Books, 2006.

Carr, Jeffrey, *Inside Cyber Warfare* (2nd ed.), (CA: O'Reilly, 2012), Chapter 18, "Active Defense for Cyber."

Cimbala, Stephen J., "Nuclear Crisis Management and Cyberwar: Phishing for Trouble," *Strategic Studies Quarterly*, (Spring 2011), pp. 117-131. http://www.au.af.mil/au/ssq/2011/spring/cimbala.pdf

Cunningham, Kevin, and Robert R. Tomes. "Space-Time Orientations and Contemporary Political-Military Thought." *Armed Forces & Society* 31, no. 1 (2004): 119-40.

Cyber Vision 2025, *United States Air Force Cyberspace Science and Technology Vision 2012-2025*, 15 July 2012.

Department of the Air Force, Air Force Policy Directive 10-17, *Cyberspace Operations*, 31 July 2012.

Department of Defense, *The Implementation of Network-Centric Warfare*, 5 January 2005.

Department of Defense, *Joint Vision 2020*. Washington DC: Government Printing Office, 2000.

Department of Defense, *Strategy For Operating In Cyberspace*, July 2011.

Dr. Kamal T. Jabbour, ST Senior Scientist Information Assurance, AF Research Laboratory, *50 Cyber Questions Every Airman Can Answer*, May 2008.

Foltz, Andrew C., Stuxnet, "Schmitt Analysis," and the Cyber "Use of Force" Debate, *Joint Forces Quarterly*, Issue 67, 4th Quarter 2012.

Gates, Bill, and Collins Hemingway. *Business @ the Speed of Thought: Using a Digital Nervous System*. New York, NY: Warner Books, 1999.

Gleick, James. *Faster: The Acceleration of Just About Everything*. New York: Pantheon Books, 1999.

Gray, Colin S. *Modern Strategy*. New York: Oxford University Press, 1999.

Habiger, Eugene E., General, USAF, retired, "Cyberwarfare and Cyberterrorism: The Need for a New US Strategic Approach," *Cyber Secure Institute* white paper no. 1:2010, 1 February 2010, 25, http://www.armytechnology.com/downloads/whitepapers/computing-software/file1552/.

Joint Publicaiton 3-09, *Joint Fire Support*, 30 June 2010.

Joint Publication 3-13, *Information Operations*, 13 February 2006.

Joint Publication 3-60, Joint Targeting, 13 April 2007.

Joint Publication 5-0, *Joint Operations Planning*, 11 August 2011.

Joint Chiefs of Staff, *Capstone Concept For Joint Operations: Joint Force 2020*, 10 September 2012.

Kugler, Richard L., "Deterrence of Cyber Attacks," *Cyberpower and National Security*, pp.309-340.
Libicki, Martin C., *Cyberdeterrence and Cyberwar* (Arlington,VA:RAND,2009),46–47,78.
LTC Scott W. Beidleman, *Defining and Deterring Cyberwar* (Carlisle, PA: Army War College, 1 June 2009), 12–13, 15.
LTG Keith Alexander, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, US Cyber Command," Senate Armed Services Committee, 14 April 10.
Maj Gen Suzanne M. Vautrinot, Department of The Air Force Presentation to The Subcommittee On Emerging Threats and Capabilities House Armed Services Committee and U.S. House of Representatives, *Improving Military Capabilities For Cyber Operations*, July 25, 2012.
Memorandum For the Secretary of Defense, *Guidance For The Preparation of The Single Integrated Operational Plan, 1963,* August 1997.
Morgan, Patrick M., Paul, T.V., and Wirtz, James J., *Complex Deterrence, Strategy in the Global Age*, The University of Chicago Press, Ltd., London, 2009.
Natural Resources Defense Council, *The U.S. Nuclear War Plan: A Time For Change*, June 2001.
Secretary of the Air Force, Chief Information Officer, *Cyberspace Operations and Support Community Transformation Plan*, 2012.
Singh, Ajay. "Time the New Dimension in War." *Joint Forces Quarterly* Winter (1995-6).
Sterner, Eric, "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly*, (Spring 2011), pp.62-80. http://www.au.af.mil/au/ssq/2011/spring/sterner.pdf
Ullman, Harlan, and James P. Wade. *Shock and Awe: Achieving Rapid Dominance*. Washington, DC: National Defense University. Institute for National Strategic Studies, 1996.
United States. Department of Defense. *Quadrennial Defense Review Report*. Washington D.C.: U.S. Government Printing Office, 2006.
United States, Joint Chiefs of Staff. *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*. [Washington, DC: Joint Chiefs of Staff : For sale by the U.S. G.P.O., Supt. of Docs.], 2004.
VADM Mike McConnell, USN, retired, "We're losing the Cyber-war. Here's the Strategy to Win It," *Washington Post*, 28 February 2010, http://www.washingtonpost.com/wp-dyn /content/article/2010/02/25/AR2010022502493.html.
Younger, Stephen M., *The Bomb A New History*, HarperCollins Publishers, New york, NY 10022, 2010.