HAKIN9 ON DEMAND

Vol.1 No.8
Issue 08/2012(8) ISSN: 1733-7186

EXPLOITING LINUX KERNEL

HOW TO HACK BIOS PASSWORD

SPECIAL PUBLICATION
80+ PAGES

HOOKING SOCKET API CALLS ON LINUX

LINUX KERNEL EXPLOIT : IS THE STORM OVER?

SECURITY POLICY DEVELOPMENT IN TRUSTED BSD MAC FRAMEWORK

CRACKING BIOS PASSWORD IN KERNEL

PLUS 2 ARTICLES ON CYBERSECURITY

Integration of

Cyberwarfare and Cyberdeterrence Strategies into the U.S. CONOPS Plan to Maximize Responsible Control and Effectiveness by the U. S. National Command Authorities

This paper deals with issues related to the present situation of lack of a clearly defined national policy on the use of cyberweapons and cyberdeterrence, as well as the urgent present need to include strategies and tactics for cyberwarfare and cyberdeterrence into the national CONOPS Plan, which is the national strategic war plan for the United States.

One of the main disadvantages of the hyper-connected world of the 21st century is the very real danger that countries, organizations, and people who use networked computer resources connected to the Internet face because they are at risk of cyberattacks that could result in one or more cyber threat dangers such as denial of service, espionage, theft of confidential data, destruction of data, and/or destruction of systems and services. As a result of these cyber threats, the national leaders and military of most modern countries have now recognized the potential for cyberattacks and cyberwar is very real and many are hoping to counter these threats with modern technological tools using strategies and tactics under a framework of cyberdeterrence, with which they can deter the potential attacks associated with cyberwarfare.

Nature of the Threat

During my studies prior to and as a student in this DET 630 – Cyberwarfare and Cyberdeterrence course at Bellevue University, it occurred to me that considering the rapid evolution of the potentially destructive capabilities of cyberweapons and the complex nature of cyberdeterrence in the 21st century, it is now a critical priority to integrate the cyberwarfare and cyberdeterrence plans into the CONOPS plan. Indeed, if the strategic battleground of the 21st century has now expanded to include cyberspace, and the U.S. has in the last five years ramped up major military commands, training, personnel, and capabilities to support cyberwarfare and cyberdeterrence capabilities, the inclusion of these capabilities should now be a critical priority of the Obama administration if has not already happened.

How large a problem is this for the United States?

Without the integration of cyberwarfare and cyberdeterrence technologies, strategies, and tactics into the CONOPS Plan, the national command authorities run a grave risk of conducting a poorly planned offensive cyberwarfare operation that could precipitate a global crisis, impair relationships with its allies, and potentially unleash a whole host of unintended negative and potentially catastrophic consequences. In non-military terms, at least four notable cyberspace events caused widespread damages via the Internet because of the rapid speed of their propagation, and their apparently ruthless and indiscriminant selection of vulnerable targets. They are 1) the Robert Morris worm (U.S. origin, 1988); 2) the ILOVEYOU worm (Philippines origin, 2000); the Code Red worm (U.S. origin, 2001); and the SQL Slammer worm (U.S. origin, 2003). If not executed with great care and forethought, a cyberweapons could potentially unleash even greater damage on intended targets and possible on unintended targets that were connected via the Internet.

Other Not So Obvious Challenges for Cyberweapons and Cyberdeterrence

The cyberspace threat and vulnerability landscape is notable in that it is continually dynamic

and shifting. Those who are responsible for protecting assets in cyberspace have many more challenges on their hands than their military counterparts who utilize weapons like guns, explosives, artillery, missiles, etc. For example, there are by some estimates over 350 new types of malware that are manufactured each month. There are also monthly patch updates to most Microsoft software and operating systems, and phenomena such as evil hackers and zero-day exploits are apparently never ending. Therefore, the inclusion of cyberweapons and cyberdeterrence capabilities into the CONOPS Plan would require more frequent, rigorous, complex, and integrated testing to ensure that it was always effective and up to date. In the dynamic world of cyberspace with its constantly shifting landscape of new capabilities, threats and vulnerabilities, the coordination of the constant refresh and testing of a CONOPS Plan that integrated these cyberwarfare and cyberdeterrence capabilities would be no small feat. In addition, constant intelligence gathering and reconnaissance would need to be performed on suspected enemies to ensure that our cyberweapons and cyberdeterrence capabilities would be in constant state of being able to deliver the intended effects for which they were designed.

Is it a problem for other countries?
The careful planning and integration of cyberweapons and cyberdeterrence is likely a challenge for every country with these capabilities. For example, much is already known about our potential adversaries, such as Russia, China and North Korea, but what is perhaps less understood is the degree to which they have been successful in integrating cyberwarfare and cyberdeterrence capabilities into their own national war plans. Nevertheless, due to the previous extensive experience of Russia and the U.S. with strategic war planning, it is more likely that each of these countries stand the greatest chance of making integrating cyberwarfare and cyberdeterrence capabilities into their respective war plans. Yet, as recently as June 2009, it was clear that the U.S. and Russia were unable to agree on a treaty that would create the terms under which cyberwarfare operations could and would be conducted (Markoff and Kramer, 2009).

Is it problematic for these countries in the same ways or is there variation? What kind?
Every country that is modern enough to have organizations, people, and assets that are connected to computers and the Internet faces similar challenges of planning and managing cyberweapons and cyberdeterrence, and the poorer the country, the more significant the challenges. For example, when a small group of hackers from Manila in the Philippines unleashed the ILOVEYOU worm on the Internet in 2000, it caused over $2 billion in damages to computer data throughout the world. Agents from the FBI went to Manila to track down these people and investigate how and why the ILOVEYOU worm catastrophe occurred. To their surprise, they learned that each of these hackers who were involved could successfully escape prosecution because there were no laws in the Philippines with which to prosecute them. So actually most countries lack the technological and legal frameworks with which to successfully build a coordinated effort to manage the weapons and strategies of cyberwarfare and cyberdeterrence, despite the fact that most now embrace cyberspace with all the positive economic benefits it offers for commerce and communications.

What are the consequences to the U.S. and others if this threat is left unchecked?
As stated earlier, without the careful integration of cyberwarfare and cyberdeterrence technologies, strategies, and tactics into the CONOPS Plan, the national command authorities run a grave risk of launching a poorly planned offensive cyberwarfare operation that could precipitate a global crisis, impair relationships with its allies, and potentially unleash a whole host of unintended negative and potentially catastrophic consequences.

What consequences has the threat already produced on American/global society?
The absence of well-defined cyberwarfare and cyberdeterrence strategies and tactics in the CONOPS Plan has already produced some situations that have either damaged America's image abroad, or that could imperil its image and have far more negative consequences. For example, operates such as Stuxnet, Flame, Duque, etc., might have either been better planned or possibly not executed at all if cyberwarfare and cyberdeterrence strategies and tactics were defined in the CONOPS Plan. Also, the news media indicated during the revolution in Libya that resulted in the fall of Qaddafi, cyberwarfare operations were considered by the Obama administration. The negative reactions and repercussions on the world stage might have far outweighed any short term advantages that could have resulted from a successful set of cyberattacks against Libyan infrastructure assets that were attached to computer networks. Again, a comprehensive CONOPS

Plan that included well-defined cyberwarfare and cyberdeterrence strategies and tactics could have prevented such possible cyberattacks from even being considered, and it could have prevented the news of the possible consideration being publicized in the press (Schmitt, E. and Shanker, T., 2011). Without such restraint and well-planned deliberate actions, the U.S. runs the risk of appearing like the well-equipped cyber bully on the world stage, and an adversary who is willing to unleash weapons that can and will do crippling damage to an opponent, using technologies that are rapid, decisive, and not well-understood by those for whom they are intended. A similar effect and world reaction might be if U.S. Army infantry troops were equipped with laser rifles that emitted deadly laser blasts with pinpoint precision across several hundred yards.

The Rapid Evolution of Cyberthreats

As predicted in the Technolytics chart below, cyberweapons have rapidly evolved over time.

Since Stuxnet was released in 2010, countries and the general public are now aware of some of the offensive, strategic and destructive capabilities and potential of cyberweapons (Gelton, T., 2011).

The changes that produced Stuxnet and other recent, more modern cyberweapons were a national resolve to excel in the cyberwarfare area, coupled with excellent reconnaissance on desired targets, and partnering with computer scientists in Israel. The political consequences are not well understood yet, except to say that the U.S. and Israel are probably less trusted and suspected of even greater future capabilities, as well as having the will to use them. Again, having well-planned cyberwarfare and cyberdeterrence strategies and tactics defined in the CONOPS Plan might indeed, restrain such possibly reckless decisions as to unleash cyberweapon attacks without what the world might consider the correct provocation.

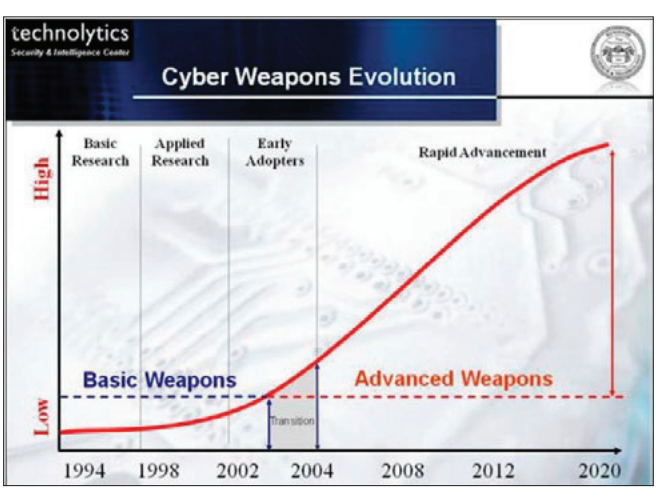

Figure 1. *Evolution of Cyberweapons (Technolytics, 2012)*

Part 1 Final Thoughts about Cyberwarfare Operations

In the words of Deb Radcliff, in an article published in SC Magazine in September 2012, "we are already in a cyberwar" (Radcliff, D., 2012). But as I was performing my research, it occurred to me that a country like the U.S., might in the future unleash such a devastating cyberattack that it could cripple the enemy's ability to communicate surrender. I think that the moral implications of such circumstances need to be justly considered as a matter of the laws of war, because if a country continues to attack an enemy that has indicated that they are defeated and want to surrender, this shifts the moral ground from which the U.S. may have it was conducting its cyberwarfare operations. This is one other unintended consequence of cyberwarfare and one that needs to be carefully considered.

Part 2 – U.S. Policy Appraisal Related to Cyberwarfare and Cyberdeterrence

This section will examine current U.S. Policy related to cyberwarfare and cyberdeterrence.

Current U.S. Policy Covering Cyberwarfare Threats

The current written policy related to cyberwarfare threats can be found in President Obama's Defense Strategic Guidance 2012, a 16-page policy documented that was published on January 3, 2012. The excerpt related specifically to cyberwarfare and cyber threats is shown below:

"To enable economic growth and commerce, America, working in conjunction with allies and partners around the world, will seek to protect freedom of access throughout the global commons – those areas beyond national jurisdiction that constitute the vital connective tissue of the international system. Global security and prosperity are increasingly dependent on the free flow of goods shipped by air or sea. State and non-state actors pose potential threats to access in the global commons, whether through opposition to existing norms or other anti-access approaches. Both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland. Growth in the number of

space-faring nations is also leading to an increasingly congested and contested space environment, threatening safety and security. The United States will continue to lead global efforts with capable allies and partners to assure access to and use of the global commons, both by strengthening international norms of responsible behavior and by maintaining relevant and interoperable military capabilities (Obama, 2012)."

The first explicit Obama Administration policy acknowledging the realities of cyber threats were published in a 30-page document titled International Strategy for Cyberspace in May 2011.

"Today, as nations and peoples harness the networks that are all around us, we have a choice. We can either work together to realize their potential for greater prosperity and security, or we can succumb to narrow interests and undue fears that limit progress. Cybersecurity is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives. While offline challenges of crime and aggression have made their way to the digital world, we will confront them consistent with the principles we hold dear: free speech and association, privacy, and the free flow of information.

"The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just, and peaceful conduct among states and peoples have begun to take hold. It is one of the finest examples of a community self-organizing, as civil society, academia, the private sector, and governments work together democratically to ensure its effective management. Most important of all, this space continues to grow, develop, and promote prosperity, security, and openness as it has since its invention. This is what sets the Internet apart in the international environment, and why it is so important to protect.

"In this spirit, I offer the United States' International Strategy for Cyberspace. This is not the first time my Administration has address the policy challenges surrounding these technologies, but it is the first time that our Nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues. And so this strategy outlines not only a vision for the future of cyberspace, but an agenda for realizing it. It provides the context for our partners at home and abroad to understand our priorities, and how we can come together to preserve the character of cyberspace and reduce the threats we face (Obama, 2011)."

Though the Obama Administration reviewed and approved President Bush's CNCI policy in May 2009, Obama, who is regarded as the most technology-savvy president that has ever occupied the White House, went much further to acknowledge the importance of cyberspace to the American economy and the American military, and the importance of defending the U.S. from adversaries that could threaten us via cyberspace. Obama's policy also acknowledges the reality that future wars will be fought on the realm of cyberspace, and has thus funded the preparation of the U.S. armed forces to prepare for conflict in cyberspace (Gerwitz, 2011).

What is the effectiveness of current policy when it concerns this particular threat issue?

The Obama Administration's policies have been effective in raising the awareness of the U.S. population as to the importance of protecting assets that are connected in cyberspace. These policies have also been effective in providing for the preparation of the U.S. military to deal with conflict in cyberspace.

However, the present policy has not been effective as a deterrence to cyber threats presented by potential national enemies and non-state actors. As recently as September 23, 2012 – September 30, 2012, cyber attacks in the form of distributed denial of service (DDOS) attacks from the Middle East against several major U.S. banks based have publicly demonstrated the ire of the attackers and also the vulnerabilities of banks with a customer presence in cyberspace (Strohm and Engleman, 2012).

Short-Term and Long-term Ramifications of Current Policy

In the short-term, the Obama Administration's policies regarding cyberspace have done much to raise the awareness of cyberspace as an area that requires protection for the public good and prosperity of the American people. These policies have also served to show our allies and our potential enemies that the U.S. has the intention of defending cyberspace and all our interests that are connected to it. In the long-term, these policies will probably evolve to reveal in a general, unclassified way,

stronger defenses, stronger deterrent capabilities and probably offensive cyberweapons.

On the legislative front, as recently as September 23, 2012, Chairman of the Senate Homeland Security Committee, Senator Joseph Lieberman (D., Connecticut), realizing that Congress would fail to pass cybersecurity legislation to designed to help protect the United States and its people, sent an urgent letter to President Obama to ask for the creation of a new Presidential Executive Order that would address several current cybersecurity issues, that includes how and when and where law enforcement can become involved in cybersecurity issues (Kerr, 2012). Though many digital privacy rights advocates, including the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the American Civil Liberties Union have strenuously fought recent cybersecurity legislation, it is expected by many cybersecurity experts that if President Obama is reelected in November 2012, an Executive Order drafted and signed by the Obama Administration provide the tools that the federal government wants. Even if President Obama is not reelected in November 2012, it is expected that some expedient action on the part of the new president would probably take place even before Congress could successfully agree upon and pass such legislation.

Allies and Adversaries Connected to this Specific Policy?

It is entirely likely that there are classified versions of the International Strategy for Cyberspace policy that address the nature of how U.S. policies regarding the defense of cyberspace will affect our allies and our adversaries. But since it has been publicly revealed that the Obama Administration has conducted offensive cyberwarfare operations against Iran between June 2009 and June 2010, it is also likely that both our allies and our enemies have a clearer understanding of U.S. capabilities as well as the intent to use cyberweapons when it deems it is in its best interests to do so.

Part 2 Conclusion

The good news is that President Obama and his Administration apparently have an acute awareness of the importance of the cyberspace to the American economy and the American military. The bad news is that because we are already in some form of cyberwarfare that appears to be rapidly escalating, it remains to be seen what effects these cyberattacks and the expected forthcoming Executive Orders that address cybersecurity will have on the American people and our way of life. Nevertheless, it will be necessary to act prudently, carefully balancing our freedoms with our need for security, and also considering the importance of enabling and protecting the prosperity of the now electronically connected, free enterprise economy that makes the U.S. the envy of and the model for the rest of the world.

Part 3 – Strategic Comparative Analysis in Cyberwarfare and Cyberdeterrence

This section will present a strategic comparative analysis of the present state of cyberwarfare and cyberdeterrence issues as that relate to other countries that could be considered adversaries, now or in the not too distant future.

What Other Countries / Regions of the World Are Concerned with This Same Threat Issue?

The countries that are primarily concerned with cyberwarfare and cyberdeterrence threat issues are the same countries that already have the greatest cyberwarfare capabilities and also the most to lose in the event of a full-scale cyberwarfare attack.

The diagram below from a 2009 study shows the comparative cyberwar capabilities of the 66 largest countries in the world.

Countries Regions of the World That Do Not Place a High Priority on This Threat Issue

Countries that are more focused on the survival and welfare of their citizens, coupled with the fact that they are largely consumers of Internet and computer capabilities versus being able to afford to channel resources into the development of cyberweapons or the resources required to develop a credible cyberdeterrence strategy. It is also ironic that the U.K. with its stature and status does not rank higher on the list shown in Table 1.

Some of the Current Policies Being Employed by These Other States / Regions in Regards to the Threat

China, Russia, and India, each of which are in the top four of the countries listed in Table 1, have well-defined cyberwarfare policies and strategies.

Cyber Military Capabilities 2009	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
China:	4.2	3.8	4.0	4.0
United States:	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.8	3.9
India:	4.0	3.5	3.5	3.7

Figure 2. *Country Cyber Capabilities Ratings (Technolytics, 2012)*

Ironically, the U.S., which occupies the number 2 position in that same table, does not yet have well-defined cyberwarfare policies and strategies. For comparison, Table 2 below shows a summary of the policies and strategies of China, Russia and India.

Successes and Failures of the Various Alternative Policies around the Globe

Despite some of the negative press from the Stuxnet virus, this collaborative effort by the U.S. and Israel has been looked at with both fascination and as an event that has quickly and successfully heralded in a new age of warfare, the age of cyberwarfare. However, many still feel that in the absence of publically defined policies and strategies by the Obama Administration, it invites a secretive and even random appearance of and the continued use of cyberweapons (Sanger, 2012).

Areas of Joint Communication / Operation / Cooperation that Exist or Should Exist Across Countries Dealing with This Threat Issue

Apparently, the U.S. has already created one or more rather sophisticated cyberweapons with the help of Israeli cyberweapon experts. At least one of these cyberweapons, the Stuxnet Worm, was effectively used to impede the development of Iran's nuclear material refinement program from 2009 to 2010 (Langer, 2010).

It is likely however, that through the auspices of the United Nations, or perhaps some G20 accord, there may be some general consensus on the importance of defining the appropriate uses cyberweapons. There also needs to be some agreement on types of response to cyberattacks, and effective methods of cyberdeterrence.

China and Its Role in Cyberwarfare Capabilities

China is probably doing a better job than the realm of cyberwarfare for three reasons: 1) the government has invested considerable resources into their cyberwarfare capabilities; 2) the number of personnel devoted to cyberwarfare efforts is reportedly in the tens of thousands; and 3) the Chinese government is able to easily operate under a cloak of secrecy and conduct operations without fear of cyberwarfare activities being leaked to Chinese press agencies (Hagestad, 2012).

Part 3 Conclusion

This paper has presented a brief strategic comparative analysis of countries with cyberwarfare capability.

Table 1. *Summary of Cyberwarfare Policies and Strategies of China, Russia, and India*

Country	Policy	Strategy
China	China supports cyberwarfare capabilities, especially providing such capabilities in the People's Liberation Army.	The Chinese will wage unrestricted warfare and these are the principles: Omni-directionality Synchrony Limited objectives Unlimited measures Asymmetry Minimal consumption Multi-dimensional coordination djustment, control of the entire process (Hagestad, 2012).
Russia	Russia supports cyberwarfare capabilities, especially providing such capabilities in the Russian Army. The nature of cyberwarfare and information warfare requires that the development of a response to these challenges must be organized on an interdisciplinary basis and include researchers from different branches – political analysts, sociologists, psychologists, military specialists, and media representatives (Fayutkin, 2012).	The ability to achieve cyber superiority is essential to victory in cyberspace. (Fayutkin, 2012).
India	India supports cyberwarfare capabilities, especially providing such capabilities in the Indian Army. "It is essential for efficient and effective conduct of war including cyber-war. The war book therefore needs to specify as how to maintain no-contact cyber war and when the government decide to go for full-contact or partial-contact war then how cyber war will be integrated to meet overall war objectives (Saini, 2012)."	Strategies are still under development, but will follow the guidance of policies related to the conduct of war. (Saini, 2012)

Part 4 – Conflict Resolution in Cyberwarfare and Cyberdeterrence

This section will present the ideas of conflict analysis and resolution as they relate to cyberwarfare.

Current Academic Research on This Threat Problem

Since 2007, as the existence of well-orchestrated cyberwar attacks such as the DDoS attacks on Estonia (2007), Georgia (2008), and Kyrgyzstan (2009), as well as the Stuxnet (2010), Duqu (2011), and Flame (2012) have all become known to the world through security researchers, their victims, and the media. As a result, it has become apparent most who are watching this area that cyberspace has now become the new realm onto which the field of international conflict has been extended, and that cyberwarfare is now no longer a theoretical issue that could one day threaten those participants and systems that rely upon connections to the Internet and Internet-connected networks. Unfortunately however, the present findings and research on cyberwarfare related events shows that the U.S. is playing catch-up and doing so badly (Turanski and Husick, 2012).

Intellectual Positions and Theoretical Explanations That Have Been Staked Out on This Threat Problem

As recently as the 2008 – 2009 timeframe, John Boyd's conflict model known as Observe – Orient – Decide – Act (OODA) began to be applied to analyze the ideas of "cybernetic warfare" and "net-centric warfare." The model itself has been analyzed for its ability to simply demonstrate the nature of the complexity of conflict, complete with factors of ambiguity, unpredictability, and so the model has also been used to define the nature of life itself. Yet, the model is also impacted by the chaotic nature of life and reality. The further shows the similarity between actual cyberwarfare events and this model. Other characteristics of the OODA loop model are its continuous nature and the feedback loops that provide data on which to base some form (or forms) of decision and action. The OODA Loop model is shown in the diagram below:

However, one key distinction between Boyd's OODA model and cybernetic warfare is Boyd's "focus on the conditions of emergence transformation of systems through information rather than merely the manner in which information is processed by a fixed organizational schema." Boyd would argue that Claude Shannon and others tend to overemphasize the view of information related to structure as opposed to information as a process (Bousquet, 2009).

Joint Publication (JP) 5-0, Joint Operation Planning

As recently as December 2006, the Joint Chiefs of Staff provided an inside look into how the U.S. National War Plan was created and maintained. In the document titled, Joint Publication (JP) 5-0, Joint Operation Planning. While this publically available, 264-page, document is unclassified, it does provide an extraordinary look into the strategic military thinking, principles, and guidance of the Joint Chiefs of Staff and the National Command Authorities as they create policies and strategies that enforce the national strategic objectives of the United States. This document that was created during the Bush administration is also significant because it is one of the first official publically known such documents that included cyberspace as part of the operational realm of conflict, along with air, sea, land, and space for conducting military operations (U.S. DoD, JCS, 2006). The high-level diagram be-

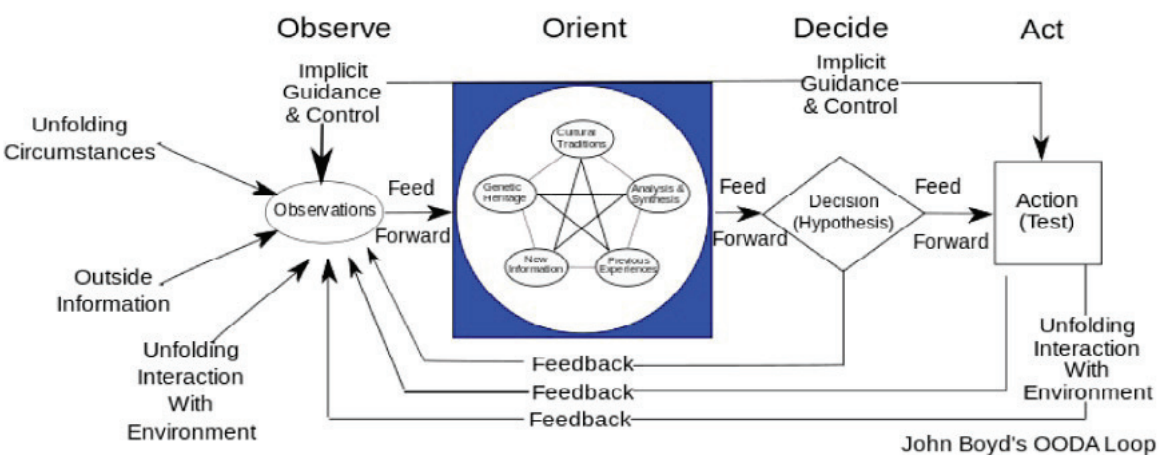

Figure 3. *Boyd's OODA Loop Model (Bousquet, 2009)*

low shows simply the concept of the inputs and the outputs that lead to understanding the operational environment of conflict, and it compares somewhat to the OODA figure shown earlier: Figure 4.

To further illustrate the intent of the Joint Chiefs of Staff to the diagram below to visually explain the interconnected nature of the realms related to the operational environment of conflict and the nature of the systems analysis required for decision making (Figure 5).

The JCS also described the environment of conflict as a place where simultaneity of operations would and this environment would include the information environment and cyberspace:

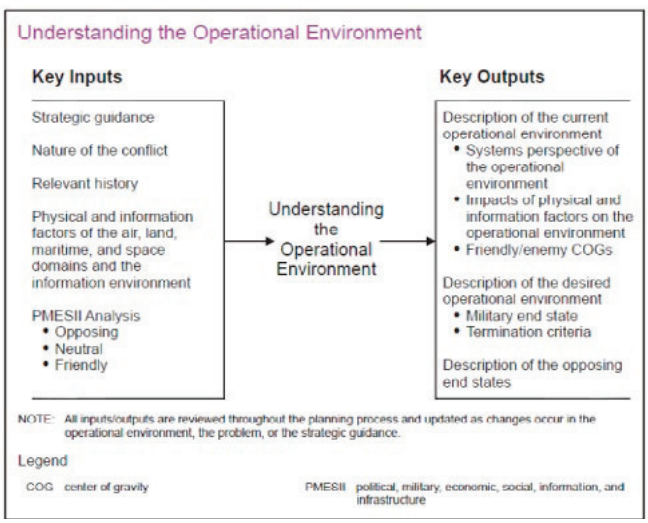

Figure 4. *Understanding the Operational Environment (U.S. DoD, JCS, 2006)*

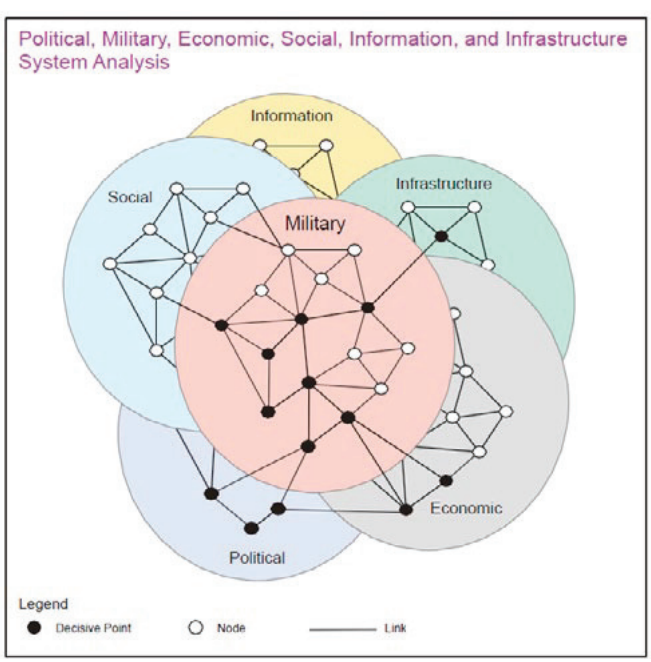

Figure 5. *Understanding the Interconnected Nature of the Realms Related to the Operational Environment of Conflict and the Nature of the Systems Analysis Required for Decision Making (U.S. DoD, JCS, 2006)*

"Simultaneity refers to the simultaneous application of military and nonmilitary power against the enemy's key capabilities and sources of strength. Simultaneity in joint force operations contributes directly to an enemy's collapse by placing more demands on enemy forces and functions than can be handled. This does not mean that all elements of the joint force are employed with equal priority or that even all elements of the joint force will be employed. It refers specifically to the concept of attacking appropriate enemy forces and functions throughout the OA (across the physical domains and the information environment [which includes cyberspace]) in such a manner as to cause failure of their moral and physical cohesion (U.S. DoD, JCS, 2006)."

Therefore, the JCS also created a Course of Action framework for determining the best courses of action in a conflict environment, and here again, cyberspace is included in that realm of options in which a course of action could and would be developed (U.S. DoD, JCS, 2006) (Figure 6).

Options in Conflict

Based on the current state of where the U.S. stands with the lack of coherent and cohesive incorporated into its National CONOPSPLAN, and the potential for unintended consequences where the unilateral use of cyberweapons can and will occur, I see three possible options for the U.S., and each of these options has advantages and disadvantages.

Part 4 Conclusion

This section has presented a brief look at the U.S. Military's recognition of cyberspace as an extension of the operational environment of conflict and

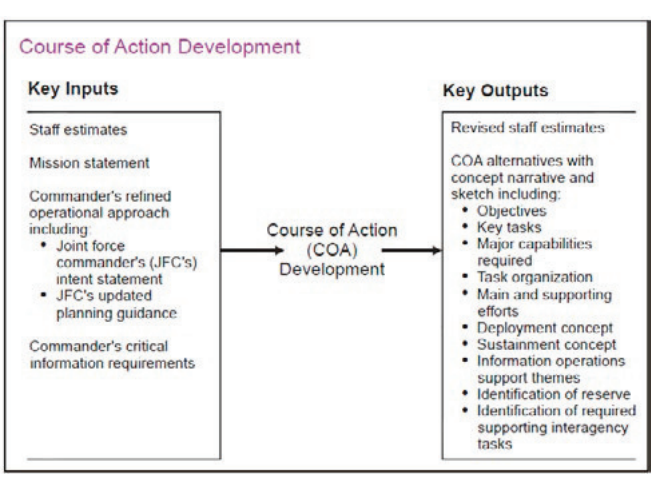

Figure 6. *Course of Action Development (U.S. DoD, JCS, 2006)*

a comparison of the options that exist for resolving the issues that threaten America's ability to create the coherent and cohesive policies and strategies that will define its ability to effectively conduct cyberwarfare and cyberdeterrence in the future.

Part 5 – Policy Generation Related to Cyberwarfare and Cyberdeterrence

This section will present the ideas for the creation of national policy or enhancement of existing national policy related to cyberwarfare and cyberdeterrence issues.

Current U.S. Policy Covering Cyberwarfare Threats

As started earlier in the Part 2 – Policy Analysis, the current written policy related to cyberwarfare threats can be found in President Obama's Defense Strategic Guidance 2012, a 16-page policy documented that was published on January 3, 2012. It has already been noted that this policy has not been effective in deterring cyberattacks and other acts of cyberwar.

Challenges Related to Cyberwar and Cyberdeterrence Policy and Strategy Creation

The creation of policies and strategies related to cyberwar and cyberdeterrence are complicated by six major issues:

- The lack of international definition and agreement on what constitutes an act of cyberwar (Markoff and Kramer, 2009).
- The lack of the ability to clearly attribute the source of an attack (Turzanski and Husick, 2012).
- The ability for non-state actors to conduct potent cyberattacks (Turzanski and Husick, 2012).
- The inability to clearly define what the exact nature of critical infrastructure targets (Turzanski and Husick, 2012).
- The massive proliferation and reliance on of ubiquitous, highly insecure, vulnerable systems based on SCADA technologies during the 1980s and 1990s (Turzanski and Husick, 2012).
- The continually changing landscape of information technology including the vulnerabilities and threats related to systems that are obsolete, yet remain in operational use for several years past their intended useful life.

A Single Integrated Operational Plan for War

During the 1950s and 1960s, when it became evident that nuclear weapons could play a major role in strategic warfare, the United States, utilized a think-tank of individuals, both military and civilian, to craft the strategic war-fighting plans of the U.S. that would deal with very real possibility that tactical and possibly strategic nuclear weapons may be required during a major wartime scenario. The first such war plan was called the Single Integrated Operational Plan (SIOP). The process of its creation involved the use of intelligence data about potential enemies, a threat assessment process, and then a process whereby the identified likely targets would be prioritized and matched with weapons. The process of matching weapons to targets also included intricate sequence timings, and the various event triggers that would result in the execution of such

Table 2. *Comparing Options for Incorporating Cyberwar and Cyberdeterrence Policies and Strategies into the U.S. National CONOPS Plan*

Option	Description	Advantage	Disadvantage
1	Create policies that mandate the inclusion of cyberwarfare and cyberdeterrence into the U.S. National CONOPS Plan	Prevents unintended consequences of unilateral use or unplanned use of cyberweapons	Takes time, politics, skills, knowledge, and money
2	Limited creation and application of policies that mandate the inclusion of cyberwarfare and cyberdeterrence into the U.S. National CONOPS Plan	Prevents some possible unintended consequences of unilateral use or unplanned use of cyberweapons	Still requires some time, political wrangling, skills, knowledge, and money
3	Do nothing whatsoever related to cyberweapons and U.S. National CONOPS Plan. Just continue to the present trend to continue to conduct cyberwarfare operations on an ad hoc basis in secrecy, and allow the situation with current cyberwarfare threats to continue (Sanger, 2012).	Saves time, political wrangling, and money	Unintended consequences of unilateral use or unplanned use of cyberweapons

attacks. In the 1980s, the SIOP evolved into something called the OPSPLAN and later, it was renamed the CONOPS Plan, but it has always been kept up to date and tested at least semiannually so that all involved would know their roles if the nation command authorities deemed it necessary to execute this intricate war plan (Freedman, 2003).

Note that as far back as the 1970s, there were 24 defined levels of conflict between the U.S. and a potential adversary, ranging from a war of words, all the way to strategic nuclear war. No matter what the name of it was, the national war plan has always been a key tool of the national command authorities for understanding what military responses would be required in the event of these various levels of conflict.

Recommendations for the U.S. Cyberwarfare Policy and Strategy

It is not unreasonable to assume that the path towards a coherent and cohesive U.S. policy and set of strategies regarding the use of cyberweapons will follow a path that is similar to the strategic war plan maturity path from Hiroshima to the SIOP. Today, in the absence of any clear policy on the use of cyberweapons, Crosston advocates the agreement on a policy of "Mutually Assured Debilitation" in which everyone with cyberweapons would come to a general understanding that the use of these weapons would result in the expectation that massive destruction would be unleashed on every participant's assets (Crosston, 2011). This makes perfect sense considering that the "Mutually Assured Destruction" nuclear deterrence policy was effective and worked well during the Cold War from the 1950s through 1990s.

Yet, today, I believe that once a coherent and cohesive U.S. policy on cyberwarfare and cyberweapons is defined by the National Command Authorities, there should be an eight-step process that could result in the development and rapid maturation of a strong national strategy U.S. Cyberwarfare:

- Define the doctrines and principles related to cyberwarfare and the needs under which cyberwarfare would be conducted.
- Create the policies that embody these doctrines and principles.
- Conduct the intelligence gathering to accurately understand the landscape of the cyber battlefield.
- Perform the analysis to create the strategy
- Create the strategic plan and tactics
- Conduct regular war games, at least twice yearly to test the strategic plan and tactics
- Analyze and document the results of the cyberwarfare war games.
- Refine the strategies and tactics for cyberwarfare and cyberdeterrence based on the results of analyzing the outcomes of the cyberwarfare war games

Note that it is also essential to continually assess the capabilities of Information Technology so that tools that our cyberwarfare fighters are using are

Table 3. *A 10-step Remedy toward the Creation of National Policy (Kramer, et al, 2009)*

Idea	Explanation
Unify Policy Direction	Effective policies will not be created by a single person or entity, but they require centralized leadership to unify their direction and intent.
Specialize Policy Direction	Recognizing that one size does not fit all, specialized policies need to be created for varies infrastructures and industries to ensure maximum protection.
Strengthen and Unify Regulation	Regulations must be strengthened to be more effective, or new, more effective regulations must be created.
Define State and Local Roles	A workable Federal policy must have the involvement of state and local authorities to be effective
Define International Interfaces	This is required because cyberspace is connected internationally and because there is still lack of international agreement on many aspects of cyberwar.
Mandate Effective Systems Engineering for Infrastructure-related Software	Ensure that there is a realization and commitment for the need to have higher minimum standards for the quality of software that is related to infrastructure.
Don't Take No for an Answer	Ensure that stakeholders and those responsible participants realize the resolute, unwavering commitment toward a workable policy solution
Establish and Implement Clear Priorities	This will ensure the best allocation of financial and management resources.
Inform the Public Clearly and Accurately	The public needs to understand the efforts being made to protect the U.S.
Conduct a Continuing Program of Research	Keep the policy updated and relevant to changing technologies.

References

- Bousquet, A. (2009). The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity. New York, NY: Columbia University Press.
- Bush, G. W. (2008). Comprehensive National Cybersecurity Initiative (CNCI). Published by the White House January 2008. Retrieved from *http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative* on January 5, 2012.
- Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.
- Clarke, R. A. and Knake, R. K. (2010). Cyberwar: the Next Threat to National Security and What to Do About It. New York, NY: HarperCollins Publishers.
- Crosston, M. (2011). World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. An article published in the Strategic Studies Quarterly, Spring 2011. Retrieved from *http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf* on October 10, 2012.
- Czosseck, C. and Geers, K. (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.
- Edwards, M. and Stauffer, T. (2008). Control System Security Assessments. A technical paper presented at the 2008 Automation Summit – A Users Conference, in Chicago. Retrieved from *http://www.infracritical.com/papers/nstb-2481.pdf* on December 20, 2011.
- Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from *http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf* on September 30, 2012.
- Freedman, L. (2003). The Evolution of Nuclear Strategy. New York, NY: Palgrave Macmillan.
- Gerwitz, D. (2011). The Obama Cyberdoctrine: tweet softly, but carry a big stick. An article published at Zdnet.com on May 17, 2011. Retrieved from *http://www.zdnet.com/blog/government/the-obama-cyberdoctrine-tweet-softly-but-carry-a-big-stick/10400* on September 25, 2012.
- Gjelten, T. (2010). Are ‚Stuxnet' Worm Attacks Cyberwarfare? An article published at NPR.org on October 1, 2011. Retrieved from *http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet* on December 20, 2011.
- Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from *http://www.npr.org/templates/story/story.php?storyId=130260413* on December 20, 2011.
- Gjelten, T. (2011). Security Expert: U.S. ‚Leading Force' Behind Stuxnet. An article published at NPR.org on September 26, 2011. Retrieved from *http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet* on December 20, 2011.
- Gjelten, T. (2011). Stuxnet Raises ‚Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011. Retrieved from *http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar* on December 20, 2011.
- Hagestad, W. T. (2012). 21st Century Chinese Cyberwarfare. Cambridgeshire, U.K.: IT Governance.
- Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.
- Jaquith, A. (2007). Security Metrics. Boston, MA: Addison Wesley.
- Kaplan, F. (1983), The Wizards of Armageddon: The Untold Story of a Small Group of Men Who Have Devised the Plans and Shaped the Policies on How to Use the Bomb. Stanford, CA: Stanford University Press.
- Kerr, D. (2012). Senator urges Obama to issue ‚cybersecurity' executive order. An article published at Cnet.com on September 24, 2012. Retrieved from *http://news.cnet.com/8301-1009_3-57519484-83/senator-urges-obama-to-issue-cybersecurity-executive-order/* on September 26, 2012.
- Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.
- Langer, R. (2010). A Detailed Analysis of the Stuxnet Worm. Retrieved from *http://www.langner.com/en/blog/page/6/* on December 20, 2011.
- Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.
- Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from *http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all* on June 28, 2009.
- Mayday, M. (2012). Iran Attacks US Banks in Cyber War: Attacks target three major banks, using Muslim outrage as cover. An article published on September 22, 2012 at Poltix. Topix.com. Retrieved from *http://politix.topix.com/homepage/2214-iran-attacks-us-banks-in-cyber-war* on September 22, 2012.
- McBrie, J. M. (2007). THE BUSH DOCTRINE: SHIFTING POSITION AND CLOSING THE STANCE. A scholarly paper published by the USAWC STRATEGY RESEARCH PROJECT. Retrieved from *http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA423774* on September 30, 2012.
- Obama, B. H. (2012). Defense Strategic Guidance 2012 – Sustaining Global Leadership: Priorities for 21st Century Defense. Published January 3, 2012. Retrieved from *http://www.defense.gov/news/Defense_Strategic_Guidance.pdf* on January 5, 2012.
- Obama, B.H. (2011). INTERNATIONAL STRATEGY for Cyberspace. Published by the White House on May 16, 2011. Retrieved from *http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf* on May 16, 2011.
- Payne, K. B. (2001). The Fallacies of Cold War Deterrence and a New Direction. Lexington, KY: The University of Kentucky Press.
- Pry, P. V. (1999). War Scare: Russia and America on the Nuclear Brink. Westport, CT: Praeger Publications.
- Radcliff, D. (2012). Cyber cold war: Espionage and warfare. An article published in SC Magazine, September 4, 2012. Retrieved from *http://www.scmagazine.com/cyber-cold-war-espionage-and-warfare/article/254627/* on September 7, 2012.
- Saini, M. (2012). Preparing for Cyberwar – A National Perspective. An article published on July 26, 2012 at the Vivikanda International Foundation. Retrieved from *http://www.vifindia.org/article/2012/july/26/preparing-for-cyber-war-a-national-perspective* on October 14, 2012.
- Sanger, D. E. (2012). Confront and Coneal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.
- Schmidt, H. S. (2006). Patrolling Cyberspace: Lessons Learned from Lifetime in Data Security. N. Potomac, MD: Larstan Publishing, Inc.

state of the art and that they are effective and perform well as they are integrated into the cyberwar war fighting environment.

Recommendations for the U.S. Cyberdeterrence Policy and Strategy

A strongly worded, explicit U.S. national policy regarding cyber deterrence would serve to further strengthen the U.S. in cyberspace as well as protect critical infrastructure and our allies. According to a 1997 paper that was prepared by the U.S. Army for the Clinton administration, Toward Deterrence in the Cyber Dimension these would be recommended elements of such a policy:

- Continue to design, create, possess, and use offensive cyber warfare capabilities when necessary
- Develop a defensive system for surveillance, assessment, and warning of a cyber attack. (I think such capability presently exists now)
- A declaration that any act of deliberate information warfare resulting in the loss of life or significant destruction of property will be met with a devastating response (U.S. Army, 1997).
- I would also include Crosston's idea of Mutually Assured Debilitation (Crosston, 2011).

Final Thoughts on the Creation of a National Policy on Cyberwar and Cyberdeterrence

According to Kramer, the table below contains the 10-step remedy for creating a policy that would protect the U.S. in cyberspace.

Part 5 Conclusion

This section has presented a brief look at the importance of creating a set of publicly available, coherent and cohesive national policies and strategies that will facilitate U.S. capabilities to effectively conduct cyberwarfare and cyberdeterrence operations now and in the future. At the present moment, the lack of such policies effectively represents a window of risk and uncertainty during a time when cyber threats and cyber attacks are growing at an exponential rate. That has the elements of a real potential for a cyber disaster if this weak policy situation is not resolved as soon as possible. Here, I presented a set of processes and a framework by which the U.S. can quickly address the national challenges of effectively creating the urgently needed national policies and integrated strategies for conducting cyberwarfare and cyberdeterrence operations now and in the future.

Conclusion

This paper has presented a brief look at the importance of creating a clear set of publicly available, coherent and cohesive national policy. It then advocated the incorporation of strategies that will address U.S. intentions and capabilities to effectively conduct cyberwarfare and cyberdeterrence operations now and in the future, into the U.S. CONOPS Plan.

References

- Schmitt, E. and Shanker, T. (2011). U.S. Debated Cyberwarfare in Attack Plan on Libya. An article published in the New York Times on October 17, 2011. Retrieved from *http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html* on October 17, 2011.
- Stiennon, R. (2010). Surviving Cyber War. Lanham, MA: Government Institutes.
- Strohm, C. and Engleman, E. (2012). Cyber Attacks on U.S. Banks Expose Vulnerabilities. An article published at BusinessWeek.com on September 28, 2012. Retrieved from *http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability* on September 30, 2012.
- Technolytics. (2012). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict, third edition. Purchased and downloaded on September 26, 2012.
- Turzanski, E. and Husick, L. (2012). "Why Cyber Pearl Harbor Won't Be Like Pearl Harbor At All..." A webinar presentation held by the Foreign Policy Research Institute (FPRI) on October 24, 2012. Retrieved from *http://www.fpri.org/multimedia/2012/20121024.webinar.cyberwar.html* on October 25, 2012.
- U.S. Army. (1997). Toward Deterrence in the Cyber Dimension: A Report to the President's Commission on Critical Infrastructure Protection. Retrieved from *http://www.carlisle.army.mil/DIME/documents/173_PCCIPDeterrenceCyberDimension_97.pdf* on November 3, 2012.
- U.S. Department of Defense, JCS. (2006). Joint Publication (JP) 5-0, Joint Operation Planning, updated on December 26, 2012. Retrieved from *http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf* on October 25, 2012.
- Waters, G. (2008). Australia and Cyber-Warfare. Canberra, Australia: ANU E Press.

WILLIAM F. SLATER, III
DET 630 – Cyberwarfare and Cyberdeterrence
Bellevue University

MATTHEW CROSSTON