Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

CYBER WARFARE: AS A FORM OF LOW-INTENSITY CONFLICT AND INSURGENCY

Samuel LILES[1]

Purdue University Calumet

Abstract: Conflict and war are inherently asymmetric in their execution and planning. As Carl von Clausewitz told us, true peer competitors would rarely engage in conflict, as mutual destruction would surely occur. Throughout the later half of the twentieth century and the first decade of the twenty-first century, wars by proxy have been the primary form of super-state conflict. The technological advantage afforded by faster communications, more accurate weapons and enhanced reconnaissance is hard to ignore. It is becoming obvious that computer network attack and defense are rising in utilization within the structure of proxy war. To add to this, the super-empowered individual and small group now have access to the same militarized technologies of cyberspace as the nation-state.

Numerous models and analogies have been suggested to explain deterrence and conflict in cyberspace. Models of real-world traditional conflict though are limited in the ability to explain how the differences of terrain and weapons translate to cyberspace. As such, a low-intensity conflict – a euphemism for guerilla warfare or insurgency – is a likely wide-spectrum conflict model that may be more appropriate. Utilizing the United States military manual on counter insurgency a discussion and comparison between ad hoc militaries and militias will be developed.

This paper serves as a point of discussion on possible models of recruitment, activities and corollaries between cyber warfare and insurgency.

Keywords: strategy, conflict, cyber warfare, insurgency, counter insurgency

[1] Purdue University Calumet, 2200 169th Street, Hammond, Indiana, 46304, United States email: liless@calumet.purdue.edu.

INTRODUCTION

How can a nation fight an asymmetric fight spanning a global commons while maintaining the respect and international reputation of the nation-state? That question, among others, is the fulcrum of discussion in this paper, while attempting to give a view into current work looking at strategies and tactics for nation-states to engage in cyber defense in a full-spectrum environment. Though not an empirical treatment, this paper should act as a stepping-stone into further discussion dealing with the substantial issue of non-state actors and statist proxies engaging in conflict on the cyber terrain.

To clarify, the position is not that low-intensity conflict is the only model that explains cyber warfare, or that insurgency is the only model that explains cyber warfare. Models and treatments have been attempted in the past to describe the cyber spectrum of conflict. A myriad group of theories and models have been suggested. While looking at deterrence, a nuclear weapons model of mutually assured destruction might be used to discuss the weaponization and deterrence issues (Libicki, 2009, p. 39). However, the use of the most powerful kinetic weapon does not answer what is basically a non-kinetic question. Other models of conflict might be considered such as strategic air power with the ability to harness substantial kinetic power (Rattray, 2001, p. 77). This too does not offer a substantial view into the non-kinetic nature of cyber warfare.

Some of the issue lies in what the effect of cyber warfare is. Parks (Parks & Duggan, 2001) says that cyber warfare needs to have a real-world impact of degrading, destroying, or disturbing to be relevant as a form of combat. This may be an interesting point but it may not be wholly the truth. The information operations spectrum is filled with case studies that suggest psychological actions may have relevancy as an associated capability to other more kinetic schemes. Both Clausewitz and Sun Tzu discuss in depth that the morale of the adversary may be broken, allowing winning without fighting (Hanzhang, 1987, p. 99), and troops need leadership once the battle has begun (Clausewitz, 1989, pp. 190-191).

The research question is whether a low-intensity conflict model, as found in insurgency/counterinsurgency, has an explanatory capability not currently found in other models of cyber conflict. As a problem for the networked force cyber conflict is not new. The concept of how to structure military units in the face of evolving threats is being considered deeper in other venues (Dion, 2004). This research in particular is meant to give a point of reference and open up dialog. It is not meant to stand alone and is expected to draw some criticism. As a work in progress, the expected path will be provided and some discussion will focus on the central thesis. Nation-states, corporate organizations and others that find they are fighting a diverse and distributed adversary will find the information provided of value. Those leading multi-national forces or organizations that are already hampered by the nature of a mission to serve across national boundaries will find significant value in the following dialog.

The United States, in 1986, with the Goldwater Nichols Act ("Goldwater Nichols Department of Defense Reorganization Act of 1986," 1986) created a new definition for conflict that was other than war and instantiated the special operations command. This became known as low-intensity conflict (LIC) and among other tenets of the Goldwater-Nichols Act providing for joint operations, it provided for a set of methods to combat small wars. There already was a "Marine Corps Small Wars" manual that dated back to 1938 and dealt with counter insurgency operations. During various conflicts the concept of counter insurgency has risen to prominence and been subjugated under a variety of policy decisions. In the American experience of Vietnam and various works on the topic of insurgency, strategies can be illuminated that inform the cyber warfare and cyber conflict spectrum. A potential answer to the research question, not expected to be the only answer, is the possibility that cyber warfare being fought by a nation-state or multi-national force is a form of counter insurgency.

1. A SPECTRUM OF CONFLICT

If we accept that cyberspace is nothing more than a new type of terrain, then the entire conflict spectrum should be found within and on that terrain. It is a principle tenet of considering the terrain of cyberspace that all of the issues of society will be found on that terrain. As humans have moved from land to sea then to space, they have taken the human condition with them. As succinctly as possible, what follows is a discussion of the spectrum of cyber conflict inclusive of cyber crime (computer and communications exploitation for criminal purposes), cyber espionage (use of networks and computer systems for spying at a nation-state or at the industrial level), cyber terrorism (using communications and computer technologies to create fear) and cyber warfare (communications and computers to supplant legitimacy or replace nation-state political structures).

1.1 CYBER CRIME

Whiteside, writing in 1978, discussed in general terms a computer crime that involved the use of computers in the earlier 1970s to misdirect railroad cars worth millions of dollars (Whiteside, 1978, p. 26). This is part of a timeline that is easy to forget, highlighting that these problems are not new and have been going on for nearly four decades. Whiteside states that in 1974 Assistant Attorney General Richard Thornburg said computer crimes came in three broad categories; 1) the computer as a victim; 2) the computer as an environment; and 3) the computer as an accomplice (Whiteside, 1978, p. 79). The technology then was only a tool. In the intervening years the model has seemingly not significantly changed.

One of the issues is that cyber crime is just crime in a new venue (cyberspace), but that it really is not new at all. Wilson argues that cyber crime is simply crime with some exceptions (Wilson, 2009, p. 417). Looking back at the discussion of different forms of crime by Thornburg, Wilson seems to be saying that the new crimes are those where the computer is the accomplice (e.g. botnets) (Wilson, 2009, p. 420). If this is true then a more holistic view of cyber crime can be taken as part of the cyberspace conflict spectrum. When looking at the incentives, it would be humorous to think that criminals would not take advantage of the computer in much the same way a shopkeeper does.

1.2 CYBER ESPIONAGE

Cyber espionage is simply espionage looking where the desired information is located. It would be silly to state that we are engaged in "file cabinet espionage" or "lockbox espionage." Lewis, discussing the incident "Titan Rain", develops a theory of cyber espionage and the issues of attribution (Lewis, 2005). As Lewis discusses, the original attribution of the espionage activities were incorrectly assessed to have originated in China. This could lead to false assumptions of attribution. Lewis cautions against jumping to conclusions too quickly. Much like darkness, the computer cloaks the spy from prying eyes, but does not mask the intruder from detection completely.

The concept of cyber espionage has a much older history found in the book by Cliff Stoll The Cuckoo's Egg (Stoll, 1990). In this case, Stoll discovered an accounting error and after many months was able to track the adversary down. This is much like regular investigations where it takes time to attribute a crime. There may be many cases of false expectations that computers will suddenly change the paradigm of investigations to a faster model.

Many authors have looked at the idea of cyber espionage, but the principle succinctly described by Lachow is that it is the use of information technology to gather information about an entity without their permission (Lachow, 2009, p. 440). In this case, Lachow is basically stating that cyber espionage is like "file cabinet espionage," but with computers and networks instead of file cabinets. Other authors have come to similar conclusions when forced to define cyber espionage. As an example, Wilson also looked at cyber espionage and follows a similar definition as Lachow (Wilson, 2009, p. 423).

1.3 CYBER TERRORISM

Verton discusses two divergent views of cyber terrorism between the professionals who are holistic in viewpoint and those who are unwilling to consider the opportunities that cyber terrorism might mean (Verton, 2003, p. 26). In many cases Verton might agree that people considering conflict are more than willing to look at a variety of the issues in an open manner. On the other hand, there are those considering conflict that have applied rule sets and are unwilling to diverge from those rule sets. This is a key insight into how insurgency is discussed later.

Quoting a definition by Mark Pollitt, Verton discusses the mistake of "pigeonholing" cyber terrorism as a primarily cyber phenomenon. The act of putting cyber terrorism in a box where it is only affecting cyber devices does not consider the larger phenomenon. A basic principle for cyber terrorism is not simply violence, but political purpose or social change in the attack. To reach a political purpose the target population must be affected in some way. As such, what Verton is discussing is that cyber terrorism is a means with results efecting human as an end.. In discussing this point, Lachow refers to cyber terrorism as the means but not the nature of the target (Lachow, 2009, p. 438). The literature is far from concrete on this issue and there are criticisms of this point. However, to consider the modes of conflict it does have an explanatory capability.

If there is cyber terrorism why do we not see it often? The argument that cyber terrorism is rare is supported by Lachow in a discussion of thousands of cyber attacks per year between 1996 and 2000 (Lachow, 2009, p. 449). With all of those attacks how many might be considered a form of terrorism? The listed attacks did not rise to the level of cyber terrorism. His assertion is that the terrorists simply were not trying or were unsuccessful in their efforts. Another point that might explain the lack of terrorism is the relationship between the adversaries. Those who might be engaged or attempting to engage in cyber terrorism simply could not create large enough effects.

2. WHY LOW-INTENSITY CONFLICT FOR CYBER WARFARE?

Low-intensity conflict is included in the conflict spectrum and used in the current networked force where cyber warfare exists. The argument over what is war and what is not war acknowledges that conflict occurs over a spectrum of action and through a variety of perception filters. The literature is rife with semantic and legal discussions on what is or is not war. The argument over different forms of "cyber" conflict has still not been answered but it has made it into the media. Whether glorifying war, creating fear in the public, or simply as a plot device there is an entire genre of cinema surrounding cyber warfare and cyber terrorism.

Conway places the blame for sensationalism surrounding cyber warfare squarely on the American entertainment industry (Conway, 2007, pp. 73–74). Conversely Leonhard, discussing the principles of information warfare says a criticism exists that argues, "*··· there can be no principles governing warfare, because each situation is unique. Hence, in the purest sense of this viewpoint, we can learn no applicable lessons, nor derive any stable truth from past military events*" (Leonhard, 1998, p. 266). Though the position of Leonhard is respected, the desire is to attempt to explain principles and strategies of cyber warfare using past practices as a model. The desire in discussing cyber warfare as a form of low-intensity conflict is not to engage in sensationalism. There is also an attempt to put cyber warfare and cyber terrorism on a continuum of conflict line as reference points.

The concept of insurgency as a form of cyber conflict is not really new. Dartnell discussed the idea of web activism and global conflict in detail. Activism can rise to the level of insurgency, but rarely takes on the full aspect of war that most people would agree with. Dartnell discusses the leveling effect that interconnected networks have had and the ability to coordinate and communicate for radicalized entities (Dartnell, 2006, p. 17). This is similar to the cyber crime example earlier in this paper. Why would activists not use the same basic tools that law enforcement might use? Adaption of the tools and dual use of tools are consistent within real world insurgencies, as we will see later.

It is interesting to see that Dartnell also suggests a tribal culture, "E-nationalism", that is being noticed (Dartnell, 2006, p. 32). When we look at the population, Kilcullen has said that "real world" insurgencies have similar patterns of behavior (Kilcullen, 2009, p. 9) in how they relate within groups. It appears in real world contemporary insurgencies, that family and tribal ties lead to political motivations rather than the inverse. Dartnell positions his argument as primarily an information domain argument rather than a kinetic argument (Dartnell, 2006, p. 25). In agreement, Maura positions the argument very similarly to Dartnell and Kilcullen in the appropriated term of "hacktivism" not being to the level of terrorism (Conway, 2007, pp. 15–17; Manion & Goodrum, 2000). Hacktivism is basically the information domain equivalent of activism leading to another semantic ambiguity.

If we consider espionage as a form of conflict less than actual warfare we have specific examples of cyber engagements by military forces. Berkowitz discusses a relevant example of what a cyber espionage engagement looks like. Two super-powers engage in conflict (United States & Russia) with the United States Navy tapping (exploiting) a cable carrying military message traffic (project code named IVY BELLS) for nearly a decade (Berkowitz, 2003, p. 56). The incident is less than war but is a military action of espionage.

Berkowitz goes on to succinctly describe the balance in adversarial use of computers as weapons, *"You can do a simple attack against a lot of computers. Or you can do a sophisticated attack against a few computers. But it is really hard to do a sophisticated attack against a lot of computers, especially an attack that would achieve a meaningful military objective"* (Berkowitz, 2003, p. 147). This is part of the equation that seems to be missing in the literature. The required effort to be highly effective is balanced by the sophistication and effect. In some ways, the amended homily, "you can have effective, simple, or numbers – pick any two", seems to work as an explanation.

When considering the relative effect, it must be balanced between the technical effect and the political effect. The elements of population, adversary and terrain within a country creates a significant environment for the population of guerilla warfare to spring up (Kilcullen, 2009, p. 41). The environment can include cyberspace, but the adversary within cyberspace does not necessarily control it. The effect is what the adversary is looking for and that is consistent with terrorism and conflict in cyberspace. On balance, it is the changes in the population's perception that gives cyber conflict power.

The role and forms of warfare within society have changed substantially. There are generational warfare constructs and they appear to be of use in explaining cyber warfare. Using a generational warfare construct, Hammes discusses how, since the end of World War II, the population centric and communications strategies have changed (Hammes, 2004, p. 33). While outside the scope of this discussion, the generational constructs give a good understanding of the perception of conflict even understanding that there are criticisms (Echevarria, 2005).

Kilcullen, writing about the Pashtun tribes said, *"… far from considering themselves part of an ordered hierarchy, members of the Pashtun tribes traditionally positioned themselves for advantage…"* (Kilcullen, 2009, p. 78). Dartnell correlates this point to the discussion on cyber activism. This correlates the concept of "real world" insurgency to the idea of cyber insurgency and thus to cyber warfare as a form of low-intensity conflict.

3. COMPARING COUNTER-INSURGENCY AND CYBER WARFARE

The United States Army and Marine Corps created a field manual to deal with counterinsurgency (FM3-24). Based on the predecessor, the *Marine Corps Small Wars Manual*, the new manual was published by Chicago University Press in 2007 (*Counterinsurgency Field Manual, 2007,* p. 2). A summary of some of the salient points will be compared and contrasted between real world counterinsurgency and cyber conflict. Having evaluated the literature surrounding the issue, a simple comparison is achieved to help guide and produce a narrative towards cyber warfare as a form of low-intensity conflict.

Considering that conflict and the precepts of war are not completely understood or agreed upon, defining the space is important even if only for this discussion. The field manual says that insurgency and counterinsurgency (COIN) are complex subsets of warfare (*Counterinsurgency Field Manual, 2007*, p. 1). The space and or terrain of this subset is not determined or even alliterated. The same discussion could then likely be used to describe piracy as much as cyber warfare.

Once the terrain and features of the conflict are accepted then the historical aspects can be considered. It is not much surprise that insurgency has a long history as a form of conflict. There is relatively nothing new about insurgency and counterinsurgency as they have been the response of populations for a long time to conflict (*Counterinsurgency Field Manual, 2007*, p. 2). Some of the first acts in negation of policy and procedures were documented by Levy in Hackers discussing the long history of activism in the cyber realm (Levy, 1984). Conflict began within the space starting with the rise of computers and internetworked components over ideology and concerns for personal safety.

As discussed by Levy, the administrative powers took action against those who were unwilling to conform. Continuing though, we see political processes that have the nation-state pitted against nonconformists in a variety of ways. Counterinsurgency fights using all of the powers of the nation-state to apply the political, military, economic, social, information and infrastructures to the population to retain legitimacy in a complex operating environment (*Counterinsurgency Field Manual, 2007*, p. 2). This is also how the various legal systems have started to react to cyberspace.

Though the legal issues are of concern, there are direct uses other than conflict that become apparent. Much like the earlier discussion on cyber crime, real world insurgents also turn to crime to fund their activities. Insurgents have used criminal enterprise to fund themselves. This allows higher freedom of action as funding is a prime vulnerability (*Counterinsurgency Field Manual, 2007,* p. 19). This adds an additional component to the consideration of the spectrum of conflict that can be traced between the real world and cyberspace.

Cyberspace is more than just information. It is the population and their perceptions about the terrain and emotional reactions to the actions taken in cyberspace. As Kilcullen said, the population is the center of gravity (Kilcullen, 2009). The field manual mentions that information as an environment is important, but it should be realized that suicide attacks and other acts have no hope of pursuing a military victory, but substantial value in undermining the legitimacy of government (*Counterinsurgency Field Manual, 2007*, p. 5). The response of counterinsurgents, or those trying to fight against insurgents, in cyberspace should be to maintain security and environments of trust. This raises the issue of information assurance and security as a larger policy question. Without the ability to provide security to people in cyberspace the legitimacy of government is suspect. These are consistent between cyberspace and real world counterinsurgencies.

The *Counterinsurgency Field Manual* specifically states some insurgent vulnerabilities, *"insurgents' need for secrecy, inconsistencies in the mobilization message, need to establish a base of operations, reliance on external support, need to obtain financial resources, internal divisions, need to maintain momentum, informants within the insurgency" (Counterinsurgency Field Manual, 2007*, pp. 31–32). A case can be made that these transfer in total between the "real world" and cyberspace. Financial concerns and security of operational activity are important in cyberspace too. Organizations that have used cyberspace for acts of war or insurgencies will require all of the same elements though they may be described differently. A question that could be asked is whether momentum remains the same between the two terrains. It would likely be attributed to similar if analogous needs.

4. CONCLUSIONS

Why have we not had a large-scale cyber war already? The question presupposes that it has not happened. There are reportedly thousands of attacks every day. They are not currently ascribed to political purposes. Looking at Clausewitz, we can see a large asymmetric advantage in the ability to make war already in place for the nation-state. In the case of the nation-state, would they respond to an act of aggression found in cyberspace via cyberspace or would they escalate to a kinetic response that the non-state actor (as an example) could not hope to survive? This kind of large-scale asymmetry has insulated the nation-states. Whether that can be maintained against an insurgency form of conflict may not be as clear. The principles of an insurgency are not to win a war, but to create a gap in credibility and legitimacy of the nation-state. In the information spectrum, insurgents posting videos of actions taken are not winning the war, but creating that inherent gap in credibility.

Another question is whether this model is too open or breaks rapidly under scrutiny. The insurgency and counterinsurgency models have withstood withering criticism but have risen and fallen as needs dictate. As a model in this simple overview, it has remained consistent and is shown to be part of the spectrum of conflict. It would be difficult to point to a cyber incident and find a better model than this one. As discussed earlier, specific case studies were not looked at within the scope of this paper. Upon publication specific case studies such as the Georgia v. South Ossetia and Estonia Cyber War could be evaluated within this lens. Case studies as part of the future work would help to cement the model. At this time though, the explanatory model has little empirical evidence to support it.

The research question is answered. The model of low-intensity conflict and specifically of insurgency and counterinsurgency does have explanatory power for cyber conflict. It may not be the only model but as a model it fits with good confidence. With future work of case study analysis, the tool may be able to differentiate between simple law enforcement and cyber warfare ends of the conflict spectrum.

BIBLIOGRAPHY

- Berkowitz, B. D., 2003. The new face of war: *How war will be fought in the 21st century*. New York: Free Press.
- Clausewitz, C. V., 1989. *On War* (Indexed ed.). Princeton: Princeton University.
- Conway, M., 2007. Cyberterrorism: Hype and reality. In L. Armistead (Ed.), *Information warfare: Separating hype from reality*. Washington, D.C.: Potomac Books.
- Dartnell, M. Y., 2006. *Insurgency online: Web activism and global conflict*. Toronto: University Toronto Press.
- Dion, E., 2004. The e-Forces!: The evolution of battle-groupings in the face of 21st century challenges. *Canadian Army Journal*(7), 3.
- Echevarria, A., 2005. Fourth-generation war and other myths. Strategic Studies Institute: United States Army War College.
- Goldwater Nichols Department of Defense Reorganization Act of 1986, 99–443 C.F.R., 1986.
- Hammes, T. X., 2004. *The sling and the stone: On war in the 21st century*. St. Paul, Mn: Zenith Press.
- Hanzhang, T., 1987. *Sun Tzu's art of war*. New York: Sterling Publishing Company.
- Kilcullen, D., 2009. *The accidental guerrilla: Fighting small wars in the midst of big ones*. Oxford: Oxford University Press.
- Lachow, I., 2009. Cyber terrorism: Menace or myth? In F. D. Kramer (Ed.), *Cyberpower and national security* (pp. 437–464). Washington D.C.: National Defense University Press.
- Leonhard, R. R., 1998. *The principles of war for the information age*. New York: Presidio Press.
- Levy, S., 1984. Hackers: *Heroes of the computer revolution*. New York: Penguin Putnam.
- Lewis, J. A., 2005. *Computer espionage, Titan Rain, and China*. Washington DC: Center for Strategic & International Studies.
- Libicki, M. C., 2009. *Cyberdeterrence and cyberwar*: RAND Corporation.
- Manion, M., & Goodrum, A., 2000. Terrorism or civil disobedience: Towards a hacktivist ethic. *Computers and Society*, June, 14–19.
- Parks, R. C., & Duggan, D. P., 2001. *Principles of cyber-warfare*. Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.
- Rattray, G. J., 2001. *Strategic warfare in cyberspace*. Cambridge: The MIT Press.
- Stoll, C., 1990. *The cuckoo's egg: Tracking a spy through the maze of computer espionage*. New York: Pocket Books.
- *The U.S. Army Marine Corps counterinsurgency field manual: US Army field manual No. 3-24 Marine Corps war-fighting publication No. 3-33.5,* 2007. Chicago: University of Chicago Press.
- Verton, D., 2003. *Black Ice: The invisible threat of cyber-terrorism.* New York: McGraw-Hill/Osborne.
- Whiteside, T., 1978. *Computer capers: Tales of electronic thievery, embezzlement, and fraud*. New York: Thomas Y. Crowell Company.
- Wilson, C., 2009. Cyber Crime. In F. D. Kramer (Ed.), *Cyberpower and national security* (pp. 415–436). Washington D.C.: National Defense University Press.