By Reverend Wylie W. Johnson, D.Min., M.Div., M.S.S.; Chaplain (Colonel), U.S. Army Reserve (Retired), Senior Pastor of Springfield Baptist Church, Springfield, Pennsylvania

Cyber is the fifth domain of warfare. It is an anonymous, global, instantaneous, virtual world not physically inhabited by persons. In cyberspace, machines are autonomous proxies for people. Humanity is removed from cyberspace by one or more orders of magnitude. It is a frontier of pure pragmatism – if it can be done, do it with a machine. Therefore the natural tendency is to view actions occurring within cyberspace as virtual and without moral content or responsibility. However, the entire field of cyberspace is a place of human endeavor that also brings with it individual and corporate human responsibility to conduct all activities ethically. All cyber actions, even second/third/fourth/etc. order effects must be evaluated for morality. Cyber War must be waged justly. Just War categories have not been rendered obsolete because the Cyber War domain is new, exponentially expanding and little understood. Rather, Just War categories are supple and comprehensive for all human undertakings in the conduct of warfare.

It is not possible to write law that anticipates every instance of human action. Enforcement of law goes a long way toward curbing the darker urges of humanity, requires highly disciplined militaries, and a national will to be virtuous. To wage a Just War requires leaders and warriors of virtue, principle and integrity. Virtue Ethics may become integral to a human being's soul, but the Law will always be an exterior value.

NEW IS OLD AND OLD IS NEW

New is old and old is new. Information has always been at the heart of warfare. What is now novel is that information is collected, transmitted and communicated at the speed of light along digital networks. The emerging field of Cyber War (CW) is rapidly developing in a largely unregulated arena where new avenues of action,[1] effects and possibilities are routinely being developed.

Cyber is the fifth domain of warfare.[2] It is a largely anonymous, global, instantaneous, virtual world—not physically inhabited by persons. In cyberspace, machines are autonomous proxies for persons. Humanity is removed from cyberspace by one or more orders of magnitude. It is a frontier of pure pragmatism. Therefore the natural tendency is to view cyberspace actions as virtual, amoral and without assignable responsibility. Cyber War is truly seductive, relatively

inexpensive, [3] and increasingly available to second and third tier nations. It has potential to harm an enemy anonymously with little chance of being identified for retribution.

Many scholars regard Cyber War as a force multiplier and not a venue for decisive warfare such as land or sea. To date this assessment is probably correct, in that without the application of conventional power a cyber-contest would not conclude hostilities. [4] However, given the immediacy, reach and relatively low cost of cyber weapons the "destructive capacity for poor and weak states is unprecedented." [5]

Cyber weapons have the potential to wreak catastrophic economic, infrastructure, and military losses while the attacking nation is insulated from retribution.

Some persons claim that Just War morality is obsolete.[6] Various arguments are put forth based upon the increasing complexity of modern warfare; or the anonymity of cyberspace; or because of the apparent demise of the Westphalian state; or because of the horrific potential of various weapons systems. Others reject the notion that Christian morality is possible. The world also recognizes the hypocrisy and frustrating futility of enforcing a morality that is reduced to a series of legal checklists.

JUST WAR APPLICABLE TO MODERN TECHNOLOGICAL ACTIONS

Just War morality, however, has not become passé. It is a matter of living virtue for both individuals and nations.[7] Virtue reaches far deeper into the human soul than professional ethics or complicity with existing laws. Virtue, or the lack of it, describes humanity. Regardless of secular optimism, human nature has not evolved beyond its fallenness. Reinhold Niebuhr wrote prolifically concerning humanity's fallenness as the appalling cause of humanity's troubles. [8]

There continues to reside within the heart of every person and the people of every nation the propensity to do evil. Therefore, virtue as personal character and moral codes guiding public and private action are essential for the maintenance of civil order. Humanity's critical social need is for a virtuous populace and leadership.

Secular societies attempt to fashion virtue and morality through the rule of law. It is not possible, however, to write law that anticipates every instance of human action. Nor is it possible to write law that changes the fundamental condition of man. At best, national and international law can

only be a guide for persons and nations that are dedicated to moral behaviors. In any case, the modern habit of substituting law for internalized morality results in a “check list” mentality and increasing disparity between the ideal and the normative. Granted, law enforcement goes a long way toward curbing the darker actions of humanity. But law is not a stand-alone; it requires a virtuous national will and an ethically disciplined military to make any meaningful difference in wartime. Virtue Ethics may become integral to a human being’s soul, but the Law will always be an exterior value. To wage a Just War necessitates leaders and warriors of virtue, principle and integrity.[9]

Just War morality is a mature and comprehensive guide for conduct of human affairs during hostilities. It is eminently applicable for the uncharted domains of Cyber War. Human beings have not somehow evolved beyond ordinary morality with the advent of the cyber domain. In fact, the reverse is true. The temptations and abilities now gathered to humanity through digital means require renewed understanding and application of moral convictions to overcome these enticements. Just War teaching demands that moral actions expressed in a networked world must be given deep thought as to their intent, content and the effects to be achieved. All human actions, cyber or otherwise, express some level of morality. To theorize that the cyber domain is amoral is a fatuous proposition.

Cyber War must be waged justly. Just War categories have not been rendered obsolete because the domain is new, exponentially expanding and little understood. The entire field of cyberspace is a place of human endeavor that also brings with it individual and corporate human responsibility toward the rest of the human race. All cyber actions, even second/third/fourth/etc. order effects must be carefully evaluated for ethical outcomes. Just War categories are supple and comprehensive for all human warfare.

TECHNOLOGICAL HERESY

Cyberwarfare supports the American war-heresy: technology supersedes all. This heresy is evidenced by commanders who focus upon information flow while ignoring the purely human element, which results in battles that are won but wars that are lost. Transactional analysis of the battlespace ignores the lessons of the past. Great Commanders of the past labored to understand their opponents and anticipate nuances that cannot be quantified.

Technological capabilities too often predetermine how they will be understood and used. Digital communication is flat and devoid of the thickness of true humanity. Complex technology lowers human attention to an unsophisticated, primal level. Concentration upon data develops commanders and formations that are unimaginative, heartless, amoral, and culturally inept warriors. America's overwhelming cyber advantage and superior intelligence production is also its most glaring weakness. Perhaps this is the primary reason Americans have consistently won battles but lost wars in the modern era. Our opponents focused upon the man, we focused upon the numbers.

Americans are in love with their technology to the point of unreality. This has to do with a faulty understanding about the nature of humanity. In spite of various science fiction fantasies, machines will never be more than tools wielded by people. Layers of complexity and function do not replace the human element, but must always guided by it. This is not *deus ex machina*, that is, personality introduced to provide a contrived solution to an apparently insoluble difficulty. Understanding the humanity of one's opponents is an honest recognition of the realities of being human.

Metaphysics and cyber war are compatible and inseparable. Ultimately the cyber effort is an expression of the human will. Imposing one's will[10] on another is a near-divine trait devolving from our creation in the *imago dei*. Remove the spiritual from the human being, and we reduce mankind to animal mechanism. Modern Western society fundamentally misunderstands the true nature of humanity. It underestimates the ontological uniqueness of homo sapiens. Only human beings can act morally or immorally, to do good or to do evil.

REMINDING OURSELVES ABOUT WHAT IS MORAL

The entire cyber domain is global in its reach, transcending sovereign borders while redefining international security.[11] It encompasses political, military, commercial, telecommunications, and civil infrastructure networks.

Cyberspace refers to the fusion of all communication networks, databases and information sources into a global virtual system and cyber-conflict is defined as cyberspace-based attacks on the civilian and military infrastructures (transportation, power, communications and financial infrastructures) upon which societies and armed forces increasingly depend.[12]

This article explores potential ways that a Just War may be conducted over cyber networks, distinguishing between Cyber War, Cyber Espionage and Cyber Attacks. Cyber War is the declared state of conflict or hostilities between two or more nations or other entities, such as an insurgent movement that is conducted over information domains. Cyber Espionage is the act of covert and unauthorized access by one nation to anther nation's computer systems, usually accomplished in a period of professed peace. Cyber Attacks[13] are the actions of a variety of non-state actors to gain unauthorized access to computers for malicious purposes.

The advent of Cyberwar (CW) is an incredible tactical development exponentially expanding the battlefield and the domain of military interest and action. What CW is not is an evolutionary leap forward that negates all that preceded it. The practitioner of the military arts must not become confused (as it were) by roiling clouds of technological smoke that obscure the effects of digital innovations. Again and again, we must remind ourselves of two principles of life. First, Christ's admonishment concerning personal culpability: "You are defiled by what comes from your heart." [14] Second, Clausewitz's dictum about taking care to act on the fundamental of war: "Everything is very simple in war, but the simplest thing is difficult." [15] New technologies for waging war can easily be mistaken for essential changes in the nature of warfare, but this is simply not so. The fundamentals of morality and the conduct of war have not changed but expanded in scope. What has changed are our ways and means of managing conflict.

Just War ethics are critical for the moral conduct of warfare. However, Western post-Christian society is increasingly without a metaphysical basis for making moral choices. Faith and war are not just compatible but inseparable. The Christian faith informs us about not only what is, but what ought to be. Morality and moral authority is always sought by humanity because we are spiritual beings; embodied souls accountable to our Creator. Faith in God gives us clear ethical reference points in the material world.

Ethical confusion arises when something like game theory[16] is substituted for ontological morality. Various choices in game theory
[17]
implicitly contain a consequentialist morality while attempting to substitute rationalized social

mechanisms for ethical choices. Whether one chooses to allow all to win or self to win is a moral choice made for larger reasons than the tactics of the moment.

Technology easily disguises moral realities. Rather than letting technology separate humanity from itself, we must more closely examine what it means to be truly human. One must always be careful to cut through the epistemological clutter. Pragmatism's fundamental mistake is to misconstrue the ontological reality of humanity. Further, refusal to recognize the necessity of universal moral principles inevitably undercuts any ethical basis for positive law. All of mankind is thus reduced to its animal state and life is conceived as purely functional.

CYBERWAR

What is Cyberwar?[18] This evolving form of conflict encompasses all digital means of information delivery that are used to attack another. CW is anonymous, autonomous, and global in its reach. The cyber realm is volatile, uncertain, complex and ambiguous (VUCA); it creates an environment filled with traps, false repositories of information, misdirection, and counterfeit identities, and severe hazards. CW is like a detective novel that mysteriously cloaks perpetrators, motives and means with a convoluted narrative. Attacks are conceived in secret, crafted in thousands of lines of code before being installed on a machine which then acts autonomously. CW is a "fire and forget" technology in which machines accomplish the bidding of absent humans.

Who wages Cyberwar? The CW realm contains a kaleidoscope of players, all acting simultaneously in the cyber drama. On low levels of the art we can identify an ill-defined cadre of independent hackers, "hacktivists" and pranksters seeking to crack various systems with malicious code, to spoof the unwary, and to steal things of worth like personal identity or trade secrets. Such persons are the matter of legend—usually portrayed as laboring over laptops in dark rooms assembling code that will bring the wicked global system to its knees.

While individual hackers can be dangerous or disruptive, they are not the real threat. Hackers are those who are picking plentiful, low-hanging digital fruit. “The majority of hackers do not have the motive or requisite tradecraft to threaten critical U.S. networks.”[19] It is well past time that we move beyond romantic notions about solitary individuals having a digitally bestowed, god-like power. Waging high-level CW today requires enormous computational power and legions of skilled code writers whose products are researched, vetted and tested in isolated networks.

CW has become the domain of well-funded nations, transnational business entities, and wealthy criminal or ideological actors. We note that CW weapons, while costly, are far more accessible and affordable than nuclear weapons or major conventional weapons systems. Further the risk of exposure for various actions, even the most egregious, is minimal unless the perpetrator reveals what was done.[20]

A limited number of nation states and well financed others have the resources to recruit well trained professionals, acquire advanced equipment and assemble enough esoteric knowledge to effectively pursue CW. A recent example of a cyber-attack made the international media. In 2010, the Chinese are widely suspected of having stolen the source code for the Google system. [21] Ordinarily, offended organizations do not publicize such thefts in order to maintain an aura of security. Public estimates of 15K (or more) daily cyber-attacks on US government systems are the visible “tip of the iceberg.” These probes and attacks come from a wide variety of sources and may simultaneously target multiple computer networks and digital systems.

A particularly nasty bit of already proliferating malicious code named STUXNET[22] infected clandestinely-acquired Iranian centrifuges that were used in the production of nuclear weapons. STUXNET involves a highly sophisticated programmable-logic-controller (PLC) rootkit
[23]
specifically targeting Siemens Industries equipment and is commonly understood to be a product of U.S.-Israeli collaboration. More recently, FLAME
[24]
, a Trojan-Horse
[25]
like program, was also discovered on Iranian computers. Again the U.S .and Israelis are generally suspected as the source for this malicious software.

The capability to go beyond the merely invasive to world-class espionage on highly secure

systems is steadily proliferating around the globe. Commercial interests are involved, seeking to uncover their rival's plans, trade secrets, and technologies. As their financial powers have exponentially grown, some criminal/ideological/religious elements are functioning in the collective CW enterprise. The obvious lure is an amazing payoff that might result in vast sums of wealth for those who successfully invade financial systems; or ruining the legitimacy of one's opponent by revealing inconvenient secrets; or causing havoc or ruin in machinery or processes; or simply identifying weaknesses to be exploited by other means.

Computational systems have gone through rapid technological development that routinely makes software and hardware superannuated in a matter of a year or less. Staying current requires an expensive and continuing parade of new software, new hardware, and new cyber-defenses. Unfortunately, government and civil infrastructure rarely keep up with this frenetic pace. Mid-to-small sized commercial interests cannot afford to stay current. Risk and vulnerability abound in essential services such as water, power generation and delivery, medical, food delivery systems and emergency services. Disruption of such delivery systems would be disastrous to any modern civilization.

AN UNREGULATED FRONTIER

The Cyber domain is a wild frontier that is governed by few laws.[26] Recently, Senator McCain led an abortive effort to pass a critical cyber-bill that would have standardized cybersecurity requirements throughout the USA.
[27]

It is an largely unregulated arena of human endeavor with a pervasive mentality that "anything goes." One is tempted to assume that the entire cyber world is a place where normal ethical-moral-legal boundaries do not apply.

The International Committee of the Red Cross (ICRC) is a vocal proponent for International Humanitarian Law (IHL)[28] that addresses attacks upon civilian infrastructure. Currently IHL only attends to the legality of cyber-attacks upon civilian infrastructure during declared conflict,
[29]

but not during periods of ostensible peace. There is, therefore, a gaping hole in international law concerning Cyber-attacks during undeclared hostilities. Looking forward, it is unlikely that there will be much international appetite for effective international or national cyber legislation in the near future. The process of developing international law and treaties is a painfully slow process, regardless of the fact that the cyber-world moves at the speed of light.

“Everything is very simple in war, but the simplest thing is difficult.”[30] Theorists have discussed and debated the reality of new generations of warfare. The simple fact is that insurgencies, guerrilla warfare, and various combinations of high and low intensity conflict have been present throughout human history. CW does not somehow afford a military commander the luxury of ignoring the essentials of war. If anything, the strategic commander must renew his focus upon the essentials of warfighting. CW adds additional layers of complexity that easily obscures Clauswitzian simplicity with both overwhelming capability and sheer information overload.

While CW encompasses a whole new set of ways (methods, tactics, and procedures) and means (various resources) for waging warfare, the ends (strategic outcomes) of war remain largely undisturbed. One must be very careful not to mistake technological advance for evolutionary changes in the fundamentals of warfare. However, CW encompasses an entirely new set of tools and heretofore unimagined possibilities for globally engaging an opponent. With these new tools comes the responsibility to use them wisely and morally.

CW is an exponential expansion of the battle-space. It offers new ways and means to engage the enemy. Gigapixel cameras[31] now under development portend a future of Orwellian oversight of entire populations. Drones and robots populate battlespace, communication is satellite enhanced, computers process information at speeds far beyond human capacity—but all these things continue to be directed by human beings. Further, it is estimated that in the next dozen years there will be “5.5 billion people online using 25 Zetabytes (trillion gigabytes) of data.”
[32]

All of these persons will soon be in the cyber cross hairs.

CW was formerly a bloodless arena of conflict but is rapidly becoming weaponized.[33] New technologies come online every day. Many of them now expand information warfare into aggressive and deadly realms. Cyber weapons currently have a deterrent value that is leveling out one-sided conflicts by increasing the transactional costs of war.
[34]

After all, how many nations would consider starting a conflict with another while facing the prospect of vital power plants being shut down, with a loss in production that could lead to a 10% (or greater) loss in GDP? Increasingly, CW is more attractive to non-state actors who have no population to please or infrastructure to protect.

Cyber-conflict is primarily disruptive, rather than destructive; and its low entry cost makes it possible for states, terrorist groups and even individuals to acquire cyber-conflict capabilities

with relative ease. Cyberspace is accessible to all and therefore makes conflict more thinkable. The less lethal appearance of cyber-conflict and the possibility of concealing the attacker's true identity (plausible deniability) put serious pressure on every war-related aspect.[35]

Increasingly, as combatants communicate digitally and operations are automated, their vulnerability to CW efforts increases. For instance, drone warfare is entirely guided by digital means, with the pilot often sitting on another side of the globe. Missiles, warplanes, smart-bombs, and other deadly devices may be guided by GPS signals originating from a network of geosynchronous satellites. Should these signals be interrupted or redirected,[36] then weapons might be turned against their users or uninvolved third parties. Recently, a high-end, highly classified intelligence U.S. RQ-170 Sentinel drone crashed in Iran while on a surveillance mission. There is some compelling evidence that Iranian malware was introduced into the Predator control network, compromising the drone and enabling the Iranians to capture the airplane nearly intact.
[37]

The very real possibility of disrupting basic civil infrastructure[38] and services has catastrophic potential for civilians who are protected as non-combatants by Just War morality. Denial of basic human services to an entire society through the disruption of civil networks brings new meaning to the concept of Total War. A civilian population might be brought to its knees by drought, famine, disease, or civil disorder by some disruptive software adroitly inserted into vulnerable control systems.

Recent cases of cyber-attacks in Estonia in April-May 2007 and Georgia in August 2008 confirm that the conflict spectrum has expanded and includes cyberspace as well (Blank2008). The Estonia cyber-attack, which primarily targeted commercial financial networks, shut down the heavily online Estonian banking system for several days. The cyber-attacks in Georgia defaced the presidential website and made other government websites unavailable. Georgia was unable to communicate on the Internet for days and relocated cyber-assets to the United States, Estonia and Poland….[39]

CW is judged such a critical battle space that the U.S. Army stood up Cyber Command, headed up by a four-star General Officer. Cyber Command will soon become a Unified Combatant Command in the U.S. military structure.[40] CW has nuanced and powerful possibilities for interaction with and response to our nation's adversaries.

In early October of this year, Harold Koh, the State Department's Chief Legal Advisor, announced U.S. Policy for Cyber Warfare.[41] Henceforth, the USA would regard certain categories of Cyber Attacks as constituting "a use of force." That particular phrase is a legal term from the charter of the United Nations that denotes the initiation of hostilities. This policy has been affirmed by Secretary of Defense Panetta in recent speeches.
[42]

Announced U.S. policy has, in fact, set a Cyber standard for the initiation of armed hostilities well ahead of the international community.

JUST WAR

How is it possible to justly wage war over cyber networks? The conduct of war must always be ethically and morally judged, for it involves the entire realm of human endeavor. Just War morality is a comprehensive ethical guide for the virtuous warrior working in extremis.

Civil and military leaders alike must not become mesmerized by the apparent moral "free fire" zone that Cyberwarfare offers. During the conduct of hostilities (jus in bello), Cyberwar like all other means of warfare must be conducted morally. Familiar and time-tested Just War categories of discrimination, proportionality, military necessity and responsibility still apply. Human actions, no matter how far removed by layers of automation, have eternal consequences. We are responsible to God for all that we do.

Unauthorized taking of property by commercial, ideological, criminal or other non-governmental entities is simply theft. There is no need to refer to Just War principle for the sanctity of property, since it is a well-established Biblical ethical principle (Exodus 20:13; Romans 13:9). Theft is also legally forbidden (even if the laws are not enforced) by every nation on the planet. It is nonsense to pretend that theft of property, intellectual or otherwise, is somehow legitimated by the necessities of the marketplace, ideology, religion, or avarice— no matter how pragmatically

satisfying the results may be to the thief.

A case for the application of Just War ethics can be made for espionage as practiced by legitimate authorities. Espionage is both an action of prevention and the prosecution of war. How does this differ from simple theft discussed above? There is a fine line here that rests upon the concept of legitimate authority. The Church Father, Augustine, expanded the teaching of the Greek Philosopher Cicero, and placed it firmly within the Christian faith. A Just War must have both Just Cause and Legitimate Authority. In International Law, “Legitimate Authority” has been identified since 1648 (the Treaty of Westphalia) as residing solely with sovereign nations. However, conflicts are rarely this simple, it usually doesn’t matter how the various sides originate when they are at war.[43] The United Nations has accorded a measure of legitimacy to insurgent and revolutionary movements by internationally recognizing their right to self-determination. [44]

Historically, when one nation is considerably stronger than its neighbors, it is inevitably lured toward conquest and empire. Espionage of national secrets has long been safety valve for nations—preventing one nation from attaining such a great advantage that it is tempted to launch a conflict. Espionage levels the playing field. For example, Ethel and Julius Rosenberg’s perfidy of divulging U.S. atomic bomb secrets to the Soviets actually had the result of militarily balancing the two superpowers for more than 40 years.

Just war ethics are deontological, that is, the ends do not justify the means—the morality of an action is not dependent on the consequences alone. So consequentialist imperative[45] “safety valve” reasoning is insufficient to make this a just war rationale. The relative anonymity, ease and safety of a cyber-penetration are pragmatic, not deontological, notions. The practicality and end results of an action are always significant, but of higher importance is the question, “is it moral?” [46]

Espionage accomplished at any time prior to hostilities is pre-emptive in nature, but may arguably be construed as a defensive action. Just War ethics recognizes the God-ordained role of government to order and defend its society (Matthew 22:21, Romans 13:1). Considering actions accomplished *Jus ad Bellum*, the Just War ethic identifies a legitimate authority’s role in preserving justice in the world under the rule of Just Cause and Right Intention. Jesus related a brief illustration about a strong man (Luke 11:21-22) and how no one would dare rob him unless there was someone stronger. In the cause of preserving justice, there is much to be gained by the international balance of powers, which has historically served as a preventative to war. So espionage done by a legitimate authority with the right intention (to maintain an equitable balance of power) for a just cause (preserving the peace) is an acceptably moral action.

Is it permissible in Just War ethics to retaliate for Cyber Attacks with conventional weapons and subsequently wage a conventional war? As noted above, the policy of the United States is to respond to certain cyber-attacks as if there were “a use of force” by another party. U.S. policy is both a warning about limitations and a notice that unspecified offensive actions would follow a cyber-attack. Can such a policy be just?

Just War morality is not a suicide pact. Serious provocations by another nation or entity may justly be met with proportionate force exercised across any or all of the five domains of war. Every nation has the moral obligation to defend its people against aggression. In the case of a cyber-attack, it is even more clear cut when the aggressor has broken either International Law or transgressed a previously announced boundary.[47] A just response may demand creativity and much thoughtful consideration, especially if the cyber-attack was aimed principally at non-combatants. A just nation would not respond simply for the need to retaliate, but responding deliberately, purposefully, and in a manner aimed at the goal of restoring a just peace.[48]

For instance, a cyber-attack on a nation’s power generation capabilities in the dead of winter would obviously be directed against the non-combatant population. But it would only marginally affect the government or military, which would have secondary, dedicated sources of power generation. Civilian lives would be in direct jeopardy, and perhaps scores of deaths would result. Thus a just response might be cyber-retaliation against the attacking nation’s banks to destabilize the national currency or a conventional military strike against governmental and military installations. The first suggested response would not place the populace in immediate physical danger, but it would certainly destabilize the government. The second possibility is a more conventional solution to the provocation and would surely result in both enemy and friendly casualties.

Such a response would satisfy the requirements for self-defense, discrimination, proportionality, military necessity and responsibility. The offended nation has a moral obligation to discriminate between combatants and non-combatants. We realize that this is not a perfect world, and there may be some non-combatants tragically intermingled with combatants— such as a baker delivering bread. However, the response is not aimed at the baker who circumstantially happened to be present but at the military node. The Just nation must deliberately choose targets based upon their military and governmental value to the enemy. Finally, the offended nation must take care to act responsibly in all of its actions, carefully weighing intent, actions and consequences.

CONCLUSION

CW is a newly developing field that may be the real revolution in military affairs. Yet, war will still consist of the fundamentals of attack and defense. As Clausewitz noted, it is simple and yet very difficult. Entry into the fifth dimension of conflict complicates decision making and actions by adding layers of complexity that may effectively distract our attention from more significant issues.

Humans remain morally accountable for their actions regardless if they pulled a trigger, launched a missile, or set a computer program into operation. The entire cyber domain is a field of human endeavor that expresses the value placed upon the moral character of all who enter there. Every action in the conduct of hostilities in any and all of the five domains of warfare must be carefully weighed as to the justness of intent, action and consequences.

Finally, Just War morality is not a checklist of good things, nor a set of legal limits, but moral principles that encompass the conduct of warfare. To live and fight justly requires Virtuous Warriors who are dedicated to justice on the contemporary frontiers of human existence.

Reverend Wylie W. Johnson serves as the Senior Pastor of Springfield Baptist Church, Springfield, Pennsylvania. Until his retirement in June 2012, he was the first Command Chaplain for the U.S. Army Military Intelligence Readiness Command.

ENDNOTES

1. Hichkad, Ravi R. & Bowie, Christopher J. Secret Weapons & Cyberwar. *Armed Forces Journal* , Gannett Government Media, Springfield, VA. June 2012, p.14ff.

2. The five domains of warfare: land, sea, air, space, cyber.

3. Cyber War is inexpensive when compared with development of nuclear weapons, or major conventional weapons systems like aircraft carriers or armor formations.

4. Rustici, Ross M. Cyberweapons: Leveling the International Playing Field. *Parameters*, Vol. XLI, No. 3, Autumn 2011. U.S. Army War College, 1222 Forbes Ave, Carlisle, PA 17013-5238, p.32.

5. *Ibid*, Rustici, p.34.

6. Bell, Daniel. The Moral Crisis of Just War: Beyond Deontology toward a Professional Military Ethic. *Journal of Faith and War*. Summer 2012, www.faithandwar.org, Monday, 02 July 2012 14:37.

7. *Ibid*, Bell.

8. Niebuhr, Reinhold. "Chapter XIII: The Case Against Pacifism." In *Reinhold Niebuhr On Politics: His Political Philosophy and Its Application to Our Age As Expressed In His Writings* , edited by Harry R. Davis & Robert C. Good. (New York: Scribner, 1960); p.147.

9. This fallacy is endemic in current American secular society which expects humans to live inclusively and harmoniously out of the goodness of their beings. In essence, it is expecting persons to live out religious virtues without the underpinnings of any sort of faith.

10. A Commander's principle task in war is to impose his or her will on the enemy.

11. Liaropoulos, Andrew. *Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict* , Academia.edu. http://piraeus.academia.edu/AndrewLiaropoulos/Papers/617962/Cyber-Security_and_the_Law_of_War_The_Legal_and_Ethical_Aspects_of_Cyber-conflict, Sept. 26, 2012.

12. *Ibid*, Liaropoulos.

13. Gorman, Siobhan and Barnes, Julian E. Iran Blamed for Cyberattacks. *The Wall Street Journal* , NY, NY. Vol. CCLX, No.88, October 13-14, 2012, p. 1.

14. Mark 7:15, New Living Translation.

15. Clausewitz, Carl Von. *On War*. Chapter 7.

16. Myerson, Roger B. Learning from Schelling's Strategy of Conflict, *Journal of Economic Literature* 2009, 47:4, 1109–1125, http:www.aeaweb.org/articles.php?doi=10.1257/jel.47.4.1109, September 24, 2012.

17. *Ibid*, Myerson.

18. It may also be labeled "information warfare," although that distinction is incomplete.

19. Buennemeyer, Timothy K. A Strategic Approach to Network Defense: Framing the Cloud. *Parameters*, Vol. XLI, No. 3, Autumn 2011. U.S. Army War College, 1222 Forbes Ave, Carlisle, PA 17013-5238, p.47.

20. Lin, Patrick; Allhoff, Fritz, & Rowe, Neil. Is It Possible to Wage a Just Cyberwar? *The Atlantic*, 19 July 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/?. Jun 5 2012.

21. http://www.geek.com/articles/mobile/chinese-ios-developer-accused-of-stealing-torchlight-assets-booted-from-app-store-20120720/

22. http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

23. A rootkit is malware code designed to hide from normal means of detection and to allow stealthy access to a computing system.

24. “Flame is the Swiss Army knife of spying tools: It can collect data entered into forms, collect passwords, record audio and capture screenshots. It may have played a reconnaissance role to scout out systems for later infection by Stuxnet, which disrupted industrial control systems made by Siemens and used by Iran for refining uranium. According to the research, Flame's command-and-control system was designed to look more like a content management system (CMS).” *Computer World*, http://www.computerworld.com/s/article/9231380/_39_Flame_39_malware_may_have_siblings_study_finds

25. A Trojan Horse is malware masquerading as a legitimate file in the computational software but is designed to allow another to have unauthorized access to the computer.

26.Rowe, Neil C. *Ethics of Cyberwar Attacks*, http://faculty.nps.edu/ncrowe/attackethics.htm, 19 July 2012

27. Fryer-Briggs, Zachary. Despite Changes, US Cyber Bill Fails, *Defense News*, Gannett Government Media, Springfield, VA., August 6, 2012, p. 30.

28. Schabas, William A. Enforcing International Humanitarian Law: Catching the Accomplices, *R ICR*
June 2001 Vol. 83 No 842, www.icrc.org/eng/assets/files/other/439-460_schabas.pdf, Sept. 21, 2012.

29. No Legal Vacuum In Cyber Space, August 16, 2011 Interview with Cordula Droege, ICRC Legal Adviser.
http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, Sept. 20, 2012.

30. *Ibid*, Clausewitz.

31. Biron, Lauren. DARPA Tests Gigapixel Cameras. *C4ISR Journal*, Gannett Government Media, Springfield, VA., August 2012, p.8.

32. Donley, Michael and Maybury, Mark. Air Force Cyber Vision 2025. *Armed Forces Journal*, October 2012. Gannett Government Media, Springfield, VA., p.22.

33. Garretson, Peter. The Case for Optionally Manned Aircraft, *Armed Forces Journal*, Gannett Government Media, Springfield, VA. Sept. 2012, pp.11ff.

34. Rustici, Ross M. Cyberweapons: Leveling the International Playing Field. *Parameters*, Vol. XLI, No. 3, Autumn 2011. U.S. Army War College, 1222 Forbes Ave, Carlisle, PA 17013-5238, p.38.

35. *Ibid*, Liaropoulos.

36. Sanborn, James K. University Demonstrates Drone Spoofing, Gannett Government Media, Springfield, VA. Sept. 2012, p10.

37. Commentary. 6 Ways to Improve UAVs. *C4ISR Journal*, Gannett Government Media, Springfield, VA., March 2012, p.30.

38. Also consider second order effects: “What may seem a precisely targeted disabling of a software module on a military computer may have profound consequences on civilian computers that happen, unknown to attackers, to use that same module.” *Ibid*, Rowe.

39. *Ibid*, Liaropoulos.

40. Fryer-Biggs, Zachary. CYBERCOM Moving Toward Command Elevation, *Defense News*, August 20, 2012.

41. Fryer-Biggs, Zachary. U.S. Moves Toward Normalization of Cyber Warfare. *Defense News*, Gannett Government Media, Springfield, VA., October 1, 2012, p.15.

42. King, Rachel. US Defense Chief Warns of Digital 9/11. *The Wall Street Journal*, October 11, 2012. (accessed October 26, 2012), http://blogs.wsj.com/cio/2012/10/11/u-s-defense-chief-warns-of-digital-911/?KEYWORDS=panetta+affirms+cyber+war+policy, internet..

43. Czege, BG Huba Wass de. "War With Implacable Foes: What All Statesmen and Generals Need to Know." *Army* 56, no. 5 (2006): 9-14.

44. It is embodied in the Charter of the United Nations and the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. Common Article 1, paragraph 1 of these Covenants provides that: "All peoples have the rights of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development." International Workgroup for Indigenous Affairs. (accessed 2009) available in http://www.iwgia.org/sw228.asp; internet.

45. Consequentialist Imperative is concerned with ends and not means, pragmatic actions and not ontology.

46. *Ibid*, Rowe.

47. Such as the new U.S. cyber policy that the USA would regard certain categories of Cyber Attacks as constituting “a use of force.”

48. The Just nation does not respond out of fear or outrage but out of a moral duty to maintain the peace. Lynn, John A. II. Fear and Outrage as Terrorist’s Goals. *Parameters*, Vol. XLII, No. 1, Spring 2011. U.S. Army War College, 1222 Forbes Ave, Carlisle, PA 17013-5238, p.51ff.