

Information Warfare and the New Challenges to Waging Just War

Matthew J. Hirschland
University of Colorado, Boulder
hirschland@hotmail.com

Revised: 7 March 2001

©2001 Matthew J. Hirschland. All rights reserved

2001 APSA Annual Meeting
San Francisco, California, USA¹

Abstract: This essay explores the implications of a new and emerging type of security threat – modern “information warfare”. It does so by examining our conceptions of what it means to wage information war (IW), appropriate responses to information attacks, and ultimately how current international laws governing the use of force are ill-equipped to address these new challenges. By employing Walzer’s formulation of “just war”, many of these problems are addressed and provocative questions are raised about the nature of security and warfare in an increasingly borderless world where states are seldom the only belligerent actors.

¹ Support was received from the Department of Political Science of the University of Colorado at Boulder.

A New Type of Security Threat

Between April 1990 and May 1991, U.S. Defense computers were compromised at 34 different locations from computers in the Netherlands. The information gleaned from these intrusions included vital information on U.S. troop movements, weapons systems, and other valuable data. So much data was accessed and downloaded that the perpetrators filled not only their own storage media, but also the pirated account space they had created on the servers of Bowling Green University and the University of Chicago. By some accounts these hackers made attempts to sell the information to Iraq's Saddam Hussein who was at the time facing a ground war with the US.¹

It is not just private “hackers” who engage in activities like those described above. Many governments also possess closely guarded and classified teams that can engage in destructive information attacks, as well as traditional espionage and eavesdropping using computers and the networks that link them together. In fact, during the 1999 conflict with Yugoslavia, the US seriously considered using its capabilities in this arena to disrupt Yugoslav military and civilian services.²

In another example of this new type of security threat, the beginnings of 1999 and 2000 saw computer viruses named “Melissa” and another endearingly termed the “Love Bug” wreak havoc upon computer systems around the world. Within three days of being reported, Melissa had reached more than 100,000 computers. The “Love Bug” virus that allegedly originated in the Philippines quickly spread, replicating itself and destroying computer files on the systems it infected, causing an estimated one billion dollars in damages before it had run its course.³

These information assaults raise interesting and challenging security and ethical questions. For example, do the Dutch hacker and email virus intrusions count as “border crossings” (whether waged by individuals or states), thus qualifying for the use of force in defensive response or at least some form of reprisal right? Additionally, how should governments who possess the ability to wage information attacks gauge and guide their use of this technology? Should the threat, and especially employment, of these

techniques be considered “acts of war” if waged by states? And if such attacks are waged by belligerent states or even belligerent *non-state* actors (NSA) and are deemed acts of war, should they then qualify under international law as eligible for a military response in retaliation?

The above episodes and the questions they raise serve first to illustrate the new threshold of terrorism and warfare upon which we stand perched. This threshold is the current and future deployment of what has been called “information operations” by the US Department of Defense (DoD), “net war” and “cyberwar” by others, but will be referred to here generally as “information warfare” (IW).⁴ These and other technological developments as they pertain to warfare have come to be referred to in general terms as the revolution in military affairs (RMA) and have dominated the security policy and armed services journals for the last decade.⁵

Second, and specifically at focus here, is the impact that these new means of terror and warfare have on our conceptions of what it means to wage “just war” and upon the international laws governing warfare that are largely rooted in conceptions of just war.⁶ Third, these episodes also highlight very real and difficult questions of where state sovereignty begins and ends in the essentially geography-free world of the Internet with computers linked across networks, and these networks linked across borders. It is these and similar questions brought about by the IW revolution that need to be addressed by mainstream academic security scholarship that has yet to effectively take up this issue, but also by international law and ultimately by our moral theories of war. The time for this is especially ripe as security studies itself comes under a more critical eye, coupled with the continued attention on the proper place for morality in our deliberations about international relations.⁷

Here I will describe the new IW technology and the challenges it poses to our thinking about security in general, the current body of international laws governing conflict, and approaches to waging just war. IW poses its greatest challenges to waging just war on two fronts: First, IW challenges traditional ideas of what constitutes “acts of war” by forcing us to reexamine our notions of “armed” conflict. Second, IW forces us to (re)define the appropriate proportionality of our employment of, and responses to such assaults and the nature of reprisal rights that are so critical to just war theory and to the formal war conventions as well. It will be demonstrated that traditional security studies itself and current international regimes *inadequately* address IW threats. Instead, it is just war theory coupled with a broadening of security studies that quite adeptly addresses *most* of these new concerns simultaneously raising new and interesting questions that require further scholarship.

Security Studies and IW

Before proceeding, a few words regarding the appropriateness of IW for security studies are in order. This is necessary since more traditional work in security studies has as its primary focus “the phenomenon of war,” which, “assumes that conflict *between states* is always a possibility.”⁸ This view articulated by Walt (1991) in his review of the field in the wake of the Cold War is representative of the state and military-centric bias of traditional security studies. This rich line of work, often realist in nature and with little regard for the morality of action, has focused on the nuclear and conventional balance of power among states.⁹ Yet with its embedded statist and military bias, this traditional scholarship of security studies has had difficulty evolving to address the new types of threats posed by the likes of IW, or has simply chosen to ignore them all together. Instead, much of the interesting and innovative work addressing IW finds its home in military, policy, and on-line journals dedicated to the subject.¹⁰

Surely, IW technologies can and do pose very real military threats that fit squarely under the more traditional rubric of security studies. Why then are they not taken up by mainstream scholarship? We could be generous here and chalk this up to the novelty of the IW threat and the slow creep of it onto the academic security agenda. It is more likely, however, that it is *not* the novelty or inappropriateness of IW for mainstream security consideration, but rather that mainstream security studies are ill-equipped to deal with the often non-military and non-state nature of the threat posed by IW.

As already highlighted, the novel use of technology employed in IW assaults to wreak havoc or “cybotage”¹¹ on the very information systems that modern states depend upon is *not always* directed at strictly military assets nor employed by state actors. As a result of this changing threat landscape, a new security paradigm is emerging to address the changing face of post-Cold War security studies by widening its scope.¹² Baldwin’s survey of the post-Cold War security literature should be viewed as a companion piece to the Walt article coming after the effects of the Cold War’s end could be better analyzed. Baldwin identifies through a survey of over fifty authors, a general trend toward a broader and not strictly military-focused notion of security studies.

Others like James Gow suggest that changes in the nature of threat today have, in fact, heralded in a “revolution in international affairs” that necessarily shifts our focus from concerns over external invasion, to those disruptions emanating from within states that disrupt international stability.¹³ IW is a prime example of these not-always-military and not-always-state centered threats that we face today. It is consideration of these new and critical threats, as well as the possible non-state origins of them, that our treatments of security must come to address. The ability of non-state actors and states alike to threaten in new ways now more than ever requires greater treatment in our journals and discourse. The study of IW is an important stride in this direction.

Information Operations Defined

For many the idea of IW is the “stuff” of science fiction. Imagine a war or assault that is won before it begins. This is a conflict in which few or no casualties are suffered by either side – an assault in which nary a shot is fired. Such an action might play out something like this:

First a computer virus is inserted by actor A into actor B’s telephone-switching stations, causing widespread failure of the telephone system. Next, computer logic bombs planted weeks earlier also by actor A and sent via seemingly innocuous e-mail, set to activate at predetermined times, destroy the electronic routers that control actor B’s rail lines and military convoys, thus mis-routing valuable military supplies and reinforcements. Meanwhile, with much of the communications network down, B’s field officers obey the only orders they see from their commander-in-chief which are on the still operating television network. Yet, the image of their leader that they see and obey is really a computer morphed and adapted phony perpetrated by actor A that commands them to lay down their arms and surrender.¹⁴

At this time, a formulation like the one above is *a bit* far-fetched and does fall within the realm of science fiction. Yet aspects of it are very real as demonstrated by the virus assaults and the use of other network debilitating information attacks. The US is the most likely state candidate to employ such techniques, yet officials from the Pentagon and the US intelligence community remain supremely guarded over actual American capabilities in this arena. With this said, the U.S. and its allies also stand to *lose* the most in an IW assault with their overwhelming preponderance of technology and dependence upon it.

The crucial components of IW that make it particularly difficult to deal with are *ambiguity, deception, and stealth*.¹⁵ The ambiguity of these attacks stems from the fact that the originating sources are often hard to trace. In terms of deception, these assaults can easily be made to look like someone else had launched them. For example, an IW assault on Indian defense computer systems could be made to look like it originated from a Pakistani source even if it really came from a hacker in Brazil. It does not take much to

imagine the potentially deadly spiral that could result from such a scenario involving these new members of the nuclear club whose enmities already run high. Last, is the element of stealth. These types of attacks can be planned and executed months in advance in a Trojan Horse manner. In the example above, the virus that attacked electronic routers of our fictitious actor B was sent via e-mail weeks in advance of the assault and sat undetected and idle until instructed to attack.

With little or no confirmation of the exact IW capabilities of states and individuals, numerous computer and infrastructure experts nevertheless treat these scenarios as very real. The fact that the US government has drafted guidelines governing the use of IW and crafted plans to deal with the consequences of an assault on American infrastructures, suggest that the threat is *real enough*.¹⁶ Some nations fearing the consequences of IW assaults have even lobbied the United Nations for legislation and a treaty governing the deployment of technology in this manner. Most prominently, it was the Russians whose foreign minister Igor Ivanov wrote Kofi Annan in October of 1999 suggesting that the effect of information weapons, “may be comparable to that of weapons of mass destruction” and proposed the creation of “international legal regimes to prohibit the development, production, or use of particularly dangerous forms of information weapons.”¹⁷ Other states have undertaken aggressive IW developmental programs as a part of their own security preparations. Recent reports on China suggest that the Chinese have embarked upon a program of IW development aimed bolstering their own IW capabilities to be used in disabling Taiwanese (ROC) communications networks as a prelude to any attempt to retake the island by force.¹⁸

With a better, albeit basic, idea of what these attacks might look like, I now turn to the elements of law and the theory of just war that undergirds those international agreements on violence that IW promises to test most severely.

The Shortcomings of International Law and the Utility of Moral Theory

As alluded to, international law and the war convention are ill-equipped to provide the answers to many of the difficult questions that IW poses (e.g. should IW assaults be deemed an act of war? What kind of reprisal rights do such attacks give? etc.). To be clear, by international law and the war convention I refer to the often disjointed, sometimes formal (and even informal) laws and agreements governing behavior leading up to and during war. In many respects, IW technology and the destructive uses to which it can be put have far out-paced our international legal institutions and agreements. We can look to bodies of law outside of the war convention for direction, but the convention itself is essentially silent on how to address these new concerns.¹⁹ Without explicit language in international regimes and the war conventions, DoD planners often turn to the rich and remarkably resilient moral theory of just war to understand the proper application and sanctioning of these new technologies.²⁰

Moral theory helps to take us a long way toward adequately answering questions like those posed above regarding the nature of IW assaults and our responses to them. For example, legal council for the DoD concluded in a recent white paper that use of IW tactics by the US in Kosovo during NATO's 1999 assault on the country would *not* be acceptable since in its deployment against Serbian military targets, no guarantee could be given that its debilitating effects would not impact civilian targets.²¹ This decision draws upon the long tradition of non-combatant immunity which is at the heart of just war theorizing and does much work in helping us to address the questions raised not only by IW, but also how to generally address the appropriate use of force.

The new practice of IW does, however, pose some immediate challenges to the age-old idea of waging a just war. The challenges posed by IW to just war do not call

into question just war theory itself, but rather the definition of war that both moral theory and international legal regimes depend upon. First, in terms of definitions, IW assaults raise questions as to whether they should be treated as “armed conflict” and “acts of war”. Second, if IW actions are indeed acts of war that merit a response, issues of proportionality and the rights of non-combatants must also be considered. I will consider each of these in turn, and then describe just how well moral theory is suited to handle them.

Definitions and Acts of War

The first question raised above is centered around definitions. Under international law, wars are initiated by border crossings or explicit declarations indicating that one state is, in fact, at war with another.²² It seems difficult to argue that an IW attack like the one in our actor A and B example above should not be defined as an act of war. However, the vast body of both formal and customary law that makes up the war convention is geared toward obvious acts of identifiable aggression that involve troops, tanks, aircraft, naval vessels, and other bits of hardware that the victim could both see and touch streaming across borders.²³ While this is certainly a shortcoming of international law, it presents only a partial problem for divining the true nature of an IW attack.

A remedy to this problem can be found in the vast body of international custom regarding sovereignty, and in other agreements codified by international regimes that go further in addressing the proper uses of communications hardware and infrastructures. Thus, custom and agreement provide some degree of protection to states when it comes to the use of these information networks for purposes other than originally intended. This, however, may be wholly inadequate when it comes to classifying IW assaults as “acts of war”. Defining “border crossing” in a networked world where information (both innocuous and pernicious) constantly crosses borders is difficult, if not impossible.

While international law is clear that true “acts of war” occur in more traditional and tangible ways with tanks, guns, bombs, and men, intuitively our scenario between actor A and B seems to strike a chord in most of us who would view such an assault as a bona fide act of war.

However, where the law is blurred, states have made crystal clear that they know exactly how IW assaults are to be treated. In a 1996 report by a DoD panel, the US Defense Science Board Task Force on Information Warfare Defense, the problem of how IW assaults will be perceived is stated bluntly: “We should not forget *information warfare is a form of warfare, not a crime or an act of terror*. . . . The response could entail civil or criminal prosecution, *use of military force*. . . diplomatic initiatives or economic mandates.’[emphasis added]”²⁴ This, taken with the Russian stance described earlier comparing IW attacks to chemical and biological weapon assaults, makes it very clear as to how IW assaults are perceived by states. That is, they plainly see them as acts of war. If what follows this reasoning is the idea that these attacks might not be *de jure* acts of war, but most certainly *de facto* acts of war, then the important question of reprisal remains to be addressed as well as our moral theory’s treatment of this type of attack.

Reprisal, Proportionality and Non-Combatants

While we may agree with the stance articulated by the US and Russians regarding IW assaults, as may many students of just war, this agreement is contingent upon the degree and nature of the IW assault. Keeping in mind that the perpetrators of IW attacks are often hard to trace, great caution must be exercised in the way we respond until we are absolutely sure who is responsible. Yet even here, a difficult question is raised: What if the perpetrator is not a state but rather an individual or group who happens to reside in the state from which the attack is launched? In our example it would be appropriate for *state B* to strike back with proportionate means, even militarily, at the

structures that enable *state A* to carry out the offensive IW operations. It would be a very different case if the U.S. launched a military assault on the home of the hackers in the Netherlands to stop them in our earlier example – or would it?

Where international law is underdeveloped and weak in addressing the questions posed by IW, moral theory is much more definitive and strong. Next, I will employ a recent formulation of just war by Michael Walzer to demonstrate that in the realm of IW, just war theory is most instructive and consistent. Just war theory also forms a solid foundation for the development of formal international conventions governing IW that should follow.

Potential Bridges and Guidance That Lie in the Moral Theory of War

Moral Theory and Definitions of War

The great strength of just war theory versus the formal war conventions is its treatment of “acts of war”. The war convention, as already noted, treats act of aggression as those tangible, physical events such as a troop crossing of a border or the dropping of a bomb. Just war, and especially Walzer’s formulation of it, also holds border crossing as the ultimate grounds for waging war under its principles of *jus ad bellum*. Yet Walzer offers a broader conception of *aggression* that better incorporates additional acts that also need to be governed by just war formulations.²⁵ In this definition aggression is, “every violation of the territorial integrity or political sovereignty of an independent state”²⁶ With this broader definition of aggression in mind, we are able to move away from ideas like “armed conflict” which frustrate potential sanctions on IW and focus on those acts that Walzer notes “challenge rights that are worth dying for.”²⁷ IW assaults very much have the ability to reach this threshold as states have already *de facto* noted, and as subsequent international law and convention must come to address. This standard of

aggression that comes from moral theory is a useful guide for how IW attacks should be perceived.²⁸

*Moral Theory on Non-Combatant Discrimination
and Questions of Proportionality*

It is on the issue of how non-combatants should be affected by IW that just war theory offers the most promising and enduring guide for behavior. As Walzer notes, non-combatants are “men and women with rights that they cannot be used for some military purpose, even if legitimate.”²⁹ These rights are to be respected by both aggressor and defender alike. With this idea of rights in mind, the injunction becomes simply: *enemy soldiers must not violate the life and liberty of enemy civilians*. Without this morally grounded understanding that is entrenched in the current war convention being carried over to cover IW, armed attacks on civilian infrastructure and civilian perpetrators would then have to be made fair game in the world of IW. Simply stated, our moral theories that cover non-combatant immunity do and must continue to apply under conditions of IW and based on DoD direction in the Kosovo case, appear to be maintained.

When it comes to non-combatant discrimination we must also address the issue of proportionality. It is here that our theory of just war begins to be more severely tested in the realm of IW. This is the case because the systems by which IW is delivered and targeted are largely dual use in nature. This means that communication networks are depended upon equally by civilian and military users alike.³⁰ Striking at them imperils the separation of combatants from non-combatants and raises serious issue over the nature and proportionality of our responses. Dr. Dan Kuehl of the National Defense University points this out in noting that with the introduction IW capabilities, we find

ourselves effectively back in the days prior to the discovery of smart weaponry such as laser and satellite guided munitions:

If Bits and Bytes offer an alternative form of exerting national power than bombs or bullets, which ethical mandate should we follow? That which attempts to hold separate the military from the civilian, no matter what the overall cost in blood and suffering, or that with attempts to minimize the destructiveness and duration of the conflict, even at the expense of affecting systems or functions that are clearly and unquestionably civilian?³¹

When forced to answer questions regarding what merits proportional and discriminatory responses to IW attacks, we are potentially lead into the fuzzy realm of the doctrine of double effect (DDE).³² A wide body of literature has sought to more clearly formulate DDE and keep us away from strictly utilitarian calculations of what is necessary to achieving war ends, while simultaneously elevating the moral component of decisions that come to impact non-combatants.³³

I will not engage in a discussion of DDE here at length, but will point out the fact that IW poses new and interesting difficulties to DDE's calculations of proportionality, intent, and discrimination that often guide the actions of belligerents in a conflict. Among these difficulties are conceptions of intent, and the nature of harm. In terms of intent, one twist that comes immediately to mind is the ability of IW to assume *non-lethal* forms like shutting off power and other infrastructure that begin to blur questions of *intent* that surround the DDE debate. Surely, one could argue that such actions will result in the death of those who rely on these infrastructures to sustain their lives (the infirmed, the elderly, etc.) thereby involving non-combatants unnecessarily.³⁴ Yet this is also one of the arenas where IW offers viable and less lethal attack options than even precise aerial or missile bombardment might provide. This, however, assumes that these IW attacks could be made to be more discriminate than traditional targeting of these infrastructures.³⁵ Second, the effects of IW can, in some of its applications, be *reversible*.

For example, with IW in its psychological form, phony commands may be given as in our example earlier, or deaths faked (like those of important leaders, prisoners, etc.) which might achieve the desired effects without inflicting *physical* harm. This element of IW raises interesting questions of whether we should differentiate physical from mental and even psychological harm. Our theories and approaches to warfare do not currently make this distinction. While I am confident that our moral theories as they have been applied to war are adequately equipped to address issues of intent that IW may raise, I am less sure that they are outfitted to address the questions of harm – especially the new types raised here.

What needs little questioning, however, is the right of states to respond in an adequate manner to such attacks that effectively neutralizes the threats they face. In keeping with moral theory's prescriptions for the right of self-defense, such responses can and will come in both conventional and informational forms of warfare. States should not be shackled in terms of the nature of their responses (conventional or IW) as long as targeting is limited to the immediate threats that are faced *even if impacting shared infrastructures*. The nature of IW attack often requires this type of response especially in those cases where shared infrastructures are employed to carry out the assaults. As a result, states that employ these dual-use infrastructures for nefarious purposes will also see these same systems suffer. However, a difficult question arises from such a prescription. This is how to handle those assaults launched by non-state actors using these same infrastructures.

Moral Theory and Reprisal Rights

Both moral theory and international convention provide some direction of how to appropriately respond to IW assaults when waged by aggressive states. For those states that are willing to engage in such attacks, are complicit in those attacks waged by groups

or individuals affiliated with them, or do not (or are unable to) take action to stop unaffiliated individuals who perpetrate them from within their borders, international law *does* provide for reprisal. As Schulman notes,

Reprisals. . . involve acts that are illegal unless they follow three steps: First, there must be an illegal act by another state. Second, the state intending to effect the reprisal must give the original assailant the opportunity to ‘make right their international wrong.’ Finally, if this demand goes unsatisfied, then the attacked party may respond *in a manner proportional to the original attack*. [Emphasis added]³⁶

The problem with international law here is twofold: First, the law is not decisive regarding the legality and nature of IW as noted earlier; and second, how should one “respond in a manner proportional to the original attack” when it is IW in nature?

Again, guidance can be found in moral theory. For Walzer, reprisal includes those acts that are “limited responses to particular transgressions,”³⁷ and seek “to break off the chain, to stop the wrongdoing *here*, with this final act [the reprisal action].”³⁸ Walzer addresses reprisals in two ways: the first is reprisal that occurs during war time as a tool of retribution like the killing prisoners of war for the acts of their comrades still engaged in the fighting, and second, reprisals during peacetime. The latter is more appropriate to our discussion of IW here and encompasses what Walzer calls the *demi-monde* – the world of raids, brief border crossings, and quick engagements that are more akin to IW concerns.

As articulated by Walzer, reprisal is, “a right, in the difficult conditions of the *demi-monde*, to seek certain effects.”³⁹ These effects must be a specific response to a specific action, must have a reasonable chance for success, and must be limited in their scope – i.e. cannot be the pretense for invasion or further military action other than what is required to neutralize the immediate threat.⁴⁰ Thus, moral theory does provide good grounding for the restoration of the *status quo ante* in the case of IW assault and

sanctions a response to them – that which is enough force to make aggressive action stop immediately and quickly return the situation to its pre-assault condition.⁴¹

Another question raised earlier that has not yet been explicitly addressed. This is what to do in those cases where it is not states but individuals or groups that launch IW assaults. Walzer is fairly clear on this front as well. He states: “if a government cannot control the inhabitants of the territory over which it supposedly presides. . .and other countries suffer because of this incapacity, then surrogate controlling and policing are clearly permissible.”⁴² He also notes that this surrogate action may “go beyond the limits commonly accepted for reprisal raids,” entailing the idea that in some cases more than just a rebuttal of the attack may be necessary to restore the *status quo ante* and the longer-term stability and security. In the case of IW, this certainly suggests a right of retribution for any such attacks that are a threat to the previously mentioned “rights worth dying for” regardless of their source. Following this mandate, it would seem *wholly appropriate* that in the case of the Dutch hackers, if the Dutch government could not stop them, then the US would possess the right to police them in a reasonable manner (e.g. destroying the network or equipment that enables their activities). However, this notion is both problematic and difficult and has the potential to further erode notions of sovereignty and territoriality in a world system of states where many governments are ill-equipped to address IW issues at large, let alone within their own borders.

Conclusions and Suggestions to Address Future IW Threats

It has been demonstrated here that the new technology of information warfare poses serious challenges to our conceptions of traditional security studies, existing international law, and especially our current war conventions. I have argued that it is the long-standing moral theory of just war that most effectively provides a starting point

from which to address these questions in a world facing increasing IW threats. These challenges raised under conditions of IW are not necessarily all new, but our answers to them must be.

Questions of discrimination, proportionality and especially notions of harm have also been raised here that require greater treatment, as do questions governing reprisal. Ultimately what is needed is the codification of our understandings of these into laws and institutions that can better address the IW threat that states pose to one another, and that non-state actors pose to the stability of the international system.⁴³ In the end, it is still just war formulations regarding how, if ever, IW should be rightly employed and responded to that must come to undergird the legitimacy of any such laws and regimes.

In the end, IW does have the potential to make wars shorter and prosecuted in much less lethal ways. However, it also democratizes warfare by making widely available this new form of aggression to those sufficiently sophisticated to use its relatively simple tools, and use them to do great harm. Like many issues surrounding the new technologies of the information age, IW raises important questions. Answers will hopefully be increasingly provided by mainstream academic work but this will only occur as the scope of security studies is widened to address these new, and often non-state-centric issues like IW. As we begin to apply the depth of knowledge from previous work detailing threat to IW questions, we are also fortunate to have a long tradition of just war theory that is useful, capable, and crucial in helping to provide morally grounded and prudent answers to these new challenges.

¹ Taken from Denning, p. 3-4.

² See Graham (1999). It ultimately chose not to do so and it was reported later that threats to use similar technologies to empty, or at least hamper, Slobodan Milosevic's access to his offshore bank accounts contributed greatly to helping end his aggression and the NATO air campaign against him. As reported by CBS's *60 Minutes*, Original air date April 9, 2000.

³ The costs associated with these attacks come primarily from time spent restoring files and cleaning out clogged e-mail systems according to ICSA.net, a computer security company that tracks the cost of computer infections.

⁴ By using the more general term "information warfare", I like Molander et al.(1998) include the concept of *both* traditional conceptions of command and control warfare (cyberwar) *and* the use of, and assault upon, the global information infrastructure (netwar) that is most often thought of as the Internet but which includes a variety of alternative information systems (banking networks, power grids, etc.).

⁵ Precision guided munitions and their impact on warfare make up a bulk of this work, but IW occupies an increasingly prominent place in this literature.

⁶ By just war, I refer to the long tradition seeking to set the moral rules of warfare. The project's aim is twofold: to govern the behavior in war when it does break out (*jus in bello*) and to set the criteria for entrance into war (*jus ad bellum*). In its modern form it justifies only wars that are: limited in scope and objective, governed by rules to protect non-combatant populations, only prosecuted to restore the status quo ante, concerned with some measure of proportionality, not fought to interfere in the domestic politics of others, and fought in self-defense.

⁷ See Walzer (1977), Roberts (1998), J. Johnson (1999), Syse (2000), and Chesterman (2001) for examples of more contemporary work in this tradition.

⁸ Walt (1991), p. 212.

⁹ Brodie (1946), Kissinger (1957), Schelling (1960), Jervis (1979), Trachtenberg, (1989), and Van Evera (1999) to name just a few.

¹⁰ It is often in journals like: *Armed Forces Journal International*, *The Naval War College Review*, *Parameters: The US Army War College Quarterly*, and online sources such as <http://www.infowar.com> that such issues are discussed.

¹¹ Taken from Arquilla et al. (1999).

¹² Articulated by such scholars as Baldwin, (1995); Katzenstein, (1996); Nye and Owens, (1996); Matthew and Shambaugh, (1998); and Buzan et al., (1998).

¹³ Gow (2000), p. 297.

¹⁴ Adapted from Douglas Waller in *Time*, August 21, 1995: Vol 146, 8.

¹⁵ As noted in Kopp (2000).

¹⁶ The US Federal government has developed a number of response teams to deal with IW attacks. These include the previously mentioned CERT, The Department of Energy's, CIAC – Computer Incident Advisory Capability, the Federal Computer Incident Response Center, the Forum of Incident Response and Security Teams, and the President's Commission on Critical Infrastructure Protection. See Denning

(1999), p. 74-75. For more on US government preparedness see: Report of the Defense Science Board Task Force on Information Warfare Defense (1996).

¹⁷ Campbell, Matthew (1998) “‘Logic Bomb’ Arms Race Panics Russia,” on InfoWar an online journal on IW. http://www.infowar.com/wmd/wmd_120898a_j.shtml

¹⁸ See Qiao and Wang (1999); Walker and Fidler (1999); Gertz (2000).

¹⁹ Space, domestic, and communications law make some provision for these questions but none are adequately answered by the crucial war conventions that help to govern behavior in times of war.

²⁰ See Johnson, Phillip A. “An Assessment of International Legal Issues in Information Operations”. Hereafter referred to as Johnson (1999).

²¹ See Graham (1999).

²² Bledsoe and Boczek (1987).

²³ As noted by Johnson (1999), p. 5.

²⁴ Brewin, Bob and Harreld, Heather, “U.S. Sitting Duck, DOD Panel Predicts,” November 11, 1996 in *Federal Computer Week* (a journal dedicated to news for the governmental IT community).

²⁵ I qualify this statement because I believe Walzer’s intent is to stick somewhat closely to the current war convention in limiting the definition of aggression. His definition, however, does lend itself to a broader and more useful interpretation that offers valuable guidance in addressing IW questions.

²⁶ Walzer, p. 52.

²⁷ *Ibid.*, p. 53.

²⁸ A 1970 General Assembly Resolution, number 2625, begins to capture this idea of ‘aggression’ by stating, “a war of aggression constitutes a crime against the peace for which there is responsibility under international law.” Yet this Resolution still incorporates the language “use of force” that has trouble explicitly addressing the IW threat. Noted by Johnson (1999), p. 13.

²⁹ Walzer, p. 137.

³⁰ Approximately 95 percent of military communications are currently routed through commercial lines. This from Berkowitz (1997) as quoted in Caldwell (1998) p. 8. Such systems include voice and data communications, power transmission grids, air-traffic control, and other vital networks.

³¹ Kuehl, p. 2-3.

³² Put simply, DDE asserts that, “an evil effect *may* be tolerated as an incident to a good effect.” Stated differently, DDE might sanction the bombardment of an active munitions factory used to prosecute a war even if “innocent” civilians may work there. It would *not* sanction carpet bombing against these civilians as they slept in their homes. In this latter case, the “good” effect is outweighed by the “evil” effect of massive civilian casualties under DDE considerations. Taken from McKenna, J. “Ethics and War: A Catholic View,” *The American Political Science Review*. Vol. 54, 3 (September 1960): 647-658.

³³ For more on DDE see: Warren Quinn “Actions, Intentions, and Consequences: The Doctrine of Double Effect,” *Philosophical and Public Affairs*. 22, 1 (Winter 1993) 334-51; Ann Davis “The Doctrine of Double Effect: Problems of Interpretation,” *Pacific Philosophical Quarterly*. 65 (1984), 107-23.

³⁴ Such actions might also arguably come to directly impact those “rights worth dying for” mentioned earlier, making them ripe for armed response and thereby accelerating the movement toward a traditional or all-out information assault.

³⁵ In other words, turning off all militarily vital infrastructure and allowing for critical exemptions for civilian operations. This might look like taking control of the power grid and allotting power only vital functions and limiting military uses of these same resources.

³⁶ Shulman (1999).

³⁷ Walzer, p. 221.

³⁸ Ibid., p. 207.

³⁹ Ibid., p. 221.

⁴⁰ Ibid., p. 220-221.

⁴¹ This suggests that this force, as long as sticking to the guidelines of jus in bello, may be either conventional or IW in nature.

⁴² Walzer., p. 220. By “surrogate controlling and policing” Walzer intends that the country suffering aggression may step in to provide the necessary correction to restore the status quo.

⁴³ A similar call for coordination efforts can be found in Denning (1999) and Libicki (1998), and in more broad terms by Matthew and Shambaugh (1998) pertaining to other transnational threats (drugs, crime, disease) and Syse (2000) as it pertains to international sanctions on violence.

REFERENCES:

- Arquilla, John; Ronfeldt, David and Zanini, Michelle. “Networks, Netwar and Information Age Terrorism,” in Lesser, Ian O. et al. (Ed.) *Countering the New Terrorism*. RAND MR-989-AF; 1999.
- Baldwin, David A. “Security Studies and the End of the Cold War,” *World Politics*. Vol. 41 (October 1995): 117-41.
- Bledsoe, Robert L. and Boczek, Boleslaw A. *The International Law Dictionary*. ABC-Clio, Inc.: Santa Barbara, CA; 1987.
- Brewin, Bob and Harreld, Heather, “U.S. Sitting Duck, DOD Panel Predicts,” November 11, 1996 in *Federal Computer Week*: <http://www.fcw.com/pubs/fcw/1111/duck.htm>.
- Brodie, B. *The Absolute Weapon*. Harcourt Brace: New York; 1946.
- Buzan, Barry; Waeber, Ole; and de Wilde, Jaap. *Security: A New Framework for Analysis*. Lynne Rienner Publishers: Boulder; 1998.
- Caldwell, Dan. “Power, Information and War,” *The Emirates Occasional Papers*. Number 15; 1998.
- Chesterman, Simon. *Just War or Just Peace: International Law and Humanitarian Intervention*. Oxford University Press; 2001.

-
- Defense Science Board Task Force on Information Warfare - Defense (IW-D), Nov. 1996, Office of the Under Secretary of Defense for Acquisition & Technology, Washington, D.C. Available at: <http://cryptome.org/iwd.htm> – Federal Computer Week.
- Denning, Dorothy E. *Information Warfare and Security*. Addison Wesley Longman, Inc: MA; 1999.
- Gertz, Bill. “Pentagon: China is preparing for high-tech war with U.S.” *Washington Times*. June 23, 2000.
- Gow, James. “A Revolution in International Affairs,” *Security Dialogue*. Vol. 31, 3 (2000): 293-306.
- Graham, Bradley “Military Grappling With Guidelines For Cyber Warfare: Questions Prevented Use on Yugoslavia,” *Washington Post*. Monday, November 8, 1999; Page A01.
- Jervis, Robert. *Perception and Misperception in International Politics*. Princeton University Press: Princeton, NJ; 1979.
- Johnson, James Turner. *Morality and Contemporary Warfare*. Yale University Press: New Haven, CT; 1999.
- Johnson, Phillip A. “An Assessment of International Legal Issues in Information Operations,” Department of Defense Office of General Counsel, May 1999: <http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc>.
- Katzenstein, Peter J. (Ed.). *The Culture of National Security: Norms and Identity in World Politics*. Columbia University Press: New York; 1996.
- Kissinger, Henry. *Nuclear Weapons and Foreign Policy*. Harper and Row: New York; 1957.
- Kopp, Carlo. Information Warfare: Part I A Fundamental Paradigm of Infowar,” *Systems – Enterprise Computing Monthly*. Feb./Mar, Auscom Publishing: Sydney, Australia; 2000. Also available at infowar.com.
- Kuehl, Dan. “The Ethics of Information Warfare and Statecraft,” National Defense University: School of Information Warfare and Strategy Paper: http://www.infowar.com/mil_c4i/mil_c4ij.html-ssi.
- Libicki Martin C., “What is Information Warfare?,” National Defense University, 1995: <http://www.ndu.edu/inss/actpubs/act003/a003cont.html>.
- Libicki, Martin C. “Information War, Information Peace,” *Journal of International Affairs*. Vol. 51,2 (Spring 1998).
- Matthew, Richard A. and Shambaugh, George E. “Sex, Drugs, and Heavy Metal: Transnational Threats and National Vulnerabilities,” *Security Dialogue*. Vol. 29, 2 (1998): 163-175.
- McKenna, J. “Ethics and War: A Catholic View,” *The American Political Science Review*. Vol. 54, 3 (September 1960): 647-658.
- Molander, Roger C., Riddile, Andrew S., and Wilson, Peter A.. “Strategic Information Warfare: A New Face of War,” *Parameters*, (Autumn 1996): 81-92.
- Molander, Roger C. and Siang, Sanyin. “The Legitimization of Strategic Information Warfare: Ethical Considerations,” *The Professional Ethics Report*. Volume XI, 4 (Fall 1998). Also available: <http://www.aaas.org/spp/dspp/sfrl/per/per15.htm>.

-
- Nye, Joseph S. and Owens, William A. "America's Information Edge," *Foreign Affairs*. (March/April 1996).
- Qiao, Liang and Wang Xiangsui. *Unrestricted Warfare*. PLA Literature and Arts Publishing House: Beijing; 1999.
- Roberts, Adam. "Implementation of the Laws of War in Late 20th Century Conflicts: Part I and II," *Security Dialogue*. Vol 29, 2 (1998): 137-150.
- Schelling, T. C. *The Strategy of Conflict*. Harvard University Press: Cambridge, MA; 1960.
- Schulman, Mark R. "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law*. Vol. 37, 3; 1999.
- Schwartz, Winn. *Cybershock : surviving hackers, phreakers, identity thieves, Internet terrorists and weapons of mass disruption*. Thunder's Mouth Press: New York; 2000.
- Syse, Henrik. "Ethics, Sovereignty, and Self-Defense: A Rejoinder," *Security Dialogue*. Vol. 31, 4 (2000): 437-442.
- Trachtenberg, M. "Strategic Thought in America, 1952-1966," *Political Science Quarterly*. Vol. 14 (1989): 301-34.
- Van Evera, S. *Causes of War: Power and the Roots of Conflict*. Cornell University Press: Ithaca; 1999.
- Walker, Tony and Fidler, Stephen. "Beijing steps up drive on computer warfare," *Financial Times*. March 16, 1999, Tuesday; p. 4.
- Walt, Stephen M. "The Renaissance of Security Studies," *International Studies Quarterly*. Vol. 35 (1991): 211-239.
- Walzer, Michael. *Just and Unjust Wars*. Basic Books: United States; 1977.
- Wei, Jincheng. "Information Warfare With Chinese Characteristics," *Jei fang jun bao* (in Chinese) *Military Forum*. June 25, 1996.