Can there be a Just Cyber War?

Michael Boylan

Marymount University, USA

Abstract

Cyber warfare is challenging traditional paradigms about what constitutes a just war. It is an emerging phenomenon that needs to be addressed separately in order to create reasonable regulations on its use and proper responses to the same. Some of these challenges refer to first what might constitute an act of war as opposed to a case of criminal sabotage. Other difficulties concern issues of sovereignty, the right to remain neutral, and proportionate responses to attack. Several recent examples of cyber-attack are brought forth and analyzed within this framework. The paper proposes that the traditional just war paradigm needs to be expanded to account for the anomalies created by this new mechanism of warfare. This essay will raise some critical questions about this changing paradigm with intent to suggest alterations to the way we think about war that can include cyber warfare as part of the traditional just war paradigm.

Key Words: Just war theory, Cyber warfare

What would happen if Heathrow's air traffic control system suddenly went down? One of the busiest airports in the world would be in sudden chaos. What would be the loss of civilian life as the scores of circling airplanes carrying hundreds of passengers each began to run into each other?[1] And what would happen if the New York Stock Exchange's computers were hit with a worm that created bogus trades on a large scale involving the trading of securities that created such a jumble that billions of dollars internationally were suddenly lost? And on a lesser scale, what if the London Eye were suddenly put into reverse mode at three times the normal pace due to a computer malfunction: a tourism disaster?

Because so much of modern life in the West is computer driven and maintained, an attack against this cyber infrastructure can have regional and international effects. It is important to examine this potentiality and how the rules of just war theory can be extended to incorporate these new dynamics.

The Traditional Paradigm

Traditionally, talk of war has been explained under the canons of "just war theory." This paradigm generally

1 Of course these scenarios are speculative since there has never been such a catastrophe before, but they were and are the fodder of security briefings. When I was with the Center for American Progress, I listened to many such scenarios from Defense experts. At the present state of the art, they are impossible completely to guard against. Various airports have had part of their systems malfunction (such as the Dublin Airport on July 9, 2008) but communications were up and they shut down the airport. The New York Stock Exchange almost yearly has some major computer failure (the latest at the writing of this essay was November 12, 2012). However, a cleaver cyber-attack would disguise itself and could potentially cause major chaos in world markets (creating a cascading effect). And though amusement park rides are engineered to high standards, several people die every year in the United States during mechanical malfunctions (http://www.rideaccidents.com/coasters.html). One can speculate what a carefully designed attack might do to a marquee ride or a general attack against ordinary rides at a given time across a country.

envisions inter-state conflicts among sovereign nations. Since the end of World War II, this paradigm has been stretched considerably until, perhaps, it is no longer accurate to describe intra-state warfare and the new technological venue of cyber warfare. We should be clear that acts of cyber sabotage occur internationally on a regular basis. The difference between sabotage and cyber warfare is a matter of degree. When you shut down a particular company for a short period of time or steal some corporate secrets or social security numbers, then we are talking about a criminal action of a minor nature. If a foreign country disabled the U.S. Navy's Seventh Fleet in such a way that it was put out of commission for an extended period of time while some other nefarious events took place that were in the jurisdiction of the Seventh Fleet, then the cyber-attack would constitute an act of war. This essay will raise some critical questions about this changing paradigm with intent to suggest alterations to the way we think about this new dimension of war.

Under the traditional paradigm war is thought to be an aggressive act by one state against the territory or sovereignty of another state for the purposes of gaining land, resources, or strategic tactical advantage according to internationally recognized rules and constraints governing such action both *ad bellum* and *in bello*.[2] The attacking state acts immorally because it *caused* the conflict. This is an important feature of the traditional paradigm respecting *ad bellum*. Of course it is often part of the public relations campaign of nation states to say that "historical aggression" or "threat" creates a compelling reason to act preemptively. These arguments were used by Hitler and George W. Bush, respectively in justifying their offensive wars to their own people. However, the principle still holds (despite those who try to employ rhetorical fallacies and lies to justify what they are doing).

Attacking states who act aggressively with their military personnel out of their own interest in a "might-makes-right" agenda can be termed *belligerent kraterists*.[3] Kraterists are those who espouse a theory of justice such that the successful exercise of power is self-justifying. I have termed this sort of distributive justice slogan, "to each according to his ability to snatch it for himself."[4] I have argued elsewhere that such a worldview is unethical.[5] But how far does one go with this assessment? General Sherman in the United States' Civil War believed that once one party violated the *ad bellum* provisions, that any *in bello* options were open to him (the one attacked unfairly).[6] But this is to mistake the difference between the reasons to *go to war* versus *the way one conducts a war*. In the traditional model these are important distinctions. Walzer, for example cites the Nazi general Rommel as doing a better job at *in bello* than the Allies' general Eisenhower (even though the Nazis fail terribly in the *ad bellum* test).[7] Thus, under the traditional paradigm there are two moral judgments to be made about the states participating in a war: (a) a judgment about origins, and (b) a judgment about how the action is carried out. War is thus constrained by rules. These rules confound the belligerent kraterist (who obeys only the rule of self-interest—hardly a moral rule at all).[8]

The traditional just war paradigm has been created over many centuries. It principally describes warfare that is between sovereign states (which have themselves evolved over time from a decentralized city-oriented structure that was based upon tribute-taxation to a more powerful roving army as a titular central authority to the modern state based upon advanced communications and ability to rapidly travel).[9] It can be tweaked to also describe civil war and guerilla war (one state which is a pretender to becoming a separate state). When we come to instances of non-state sponsored terrorism, the model is shakier. The line between criminal activity and non-state sponsored terrorism is blurry at best.[10]

Another set of key understandings in the traditional paradigm concerns what war consists of in practice. Certainly in the earliest times war was a gang fest in which the well-conditioned warriors won the day. This does not mean that tactics (such as the phalanx in the Battle of Marathon) and weapons (such as Alexander's long spears) were not important, but the most critical element was well-conditioned *arête* soldiers.[11] Aristotle certainly thought about it in this way in his depiction

2 There are, of course, various sources of just war theory. One good overview of these can be found in Gregory M. Reichberg, Henrik Syse, and Endre Begby. Here and elsewhere I also use Michael Walzer as a representative of the traditional paradigm cannon.

3 Boylan (2011): 177.

4 Boylan (2004): 145.

5 Boylan (2004): 151-153.

6 Walzer (1977): 32-33.

7 Walzer (1977): 37-38.

8 One critic of the traditional model as set out by Walzer is Jeff McMahan, "The Ethics of Killing in War" *Ethics* 114.4 (2004): 693-733. McMahan characterizes the issue as: "Let us say that those who fight in a just war are 'just combatants,' while those who fight in a war that is unjust because it lacks a just cause are 'unjust combatants' " (693).

9 For a good description of the ancient polity see: James Romm, *Ghost on the Throne: The Death of Alexander the Great and the War for the Crown and Empire.* (N.Y.: Knopf, 2011).

10 Boylan (2011): ch. 13.

11 On the use of the phalanx see Peter Krentz, *The Battle of Marathon* (New Haven, CT: Yale University Press, 2011). Discussion of Alexander's weapons can be found in Romm, *op.cit.*

of slavery in the *Politics*.[12] Though the argument is proximately about slavery, the underlying background conditions address what he felt war was about.

1. War may be just or unjust—Fact
2. In just wars virtue and excellence make for winning—Assertion
3. Virtue and excellence are marks of masters—Assertion
4. In just wars, losers are properly slaves—2, 3
5. In unjust wars virtue and excellence may not account for winning—1, 2
6. In unjust wars slavery may also be unjust—4, 5

Aristotle thought that *arête* for warriors consisted in being the strongest and endowed with the most fortitude. Thus the winning side *deserved* to win. Those on the losing side *deserved* to be subjugated (so long as there was no trickery and the outcome was decided by strength and conditioning).

But technology and innovation had a way of changing this rather athletic depiction of warfare. Various advances in armor, cavalry, long bows and cross bows, gun powder, the confluence of WWI alterations (airplanes, poisonous gas, accurate heavy artillery, et al), and the fine tuning of these alterations with new addition of the ultimate technical innovation—the atomic bomb in WWII. The result of all of this is a permanent alteration of the traditional paradigm in significant ways. Though it is still a contest, the technology of today allows the side with the most powerful weapons to possess a tremendous advantage *ceteris paribus* over an opponent who is more physically fit, but less well armed.

Cyber Warfare

The most modern technological advancements in warfare include robotic warfare and cyber warfare. This essay will concentrate upon the latter as it stretches the traditional paradigm significantly. This is because: (a) The role of killing— in the traditional paradigm this is part of the deal, but in cyber warfare killing (though it may occur) is not primary, (b) Attribution—it is not always clear who committed the act (cf. Duqu, Stuxnet, and Flame), (c) Territoriality and neutrality are blurred as internet hubs go everywhere, (d) The conceptualization of the attack and response need new clarification. Let's address these in order.

Alterations to the Traditional Paradigm

First, there is the change to the normal way we think of what constitutes an *act of war*.[13] Earlier I suggested that it was an aggressive act by one state against the territory or sovereignty of another state for the purposes of gaining land, resources, or strategic advantage according to internationally recognized rules and constraints governing such action both *ad bellum* and *in bello*. Well, this traditional understanding requires at least two components: 1. An aggressive act by one state against another against its territory or sovereignty, and 2. A *telos* of gaining land, resources, or strategic advantage. A traditional understanding of the first point envisions military personnel moving into a region to take control—involving almost universally the loss of life (preferably military only).[14] In a cyber-attack there are no ground troops. The delivery mechanism is either via the Internet or by the agency of a fifth column person who has malware on a flash drive (the probable launch of Stuxnet).

Among the sorts of attacks there is the *virus* (malware that attaches itself to another file, program, or e-mail) and it replicates (as in Duqu and Flame). This sort of attack is so general in scale that it would affect not only the target country but any other country connected by the Internet (presuming that the attack is not Intranet). Because of this widespread feature of the virus, it is impossible to preserve the military v. civilian distinction common to just war theory.[15]

A second sort of attack is a *worm*. It is a free standing program that can be more targeted (like the Stuxnet worm). This might be the malware of choice for the near-term cyber war arsenal. Because there can be firewalls established against worms, the best delivery device is via a flash drive inserted into the Inter- or Intranet system by a spy or fifth column individual. This requires subterfuge entry into the sovereignty of another country to perform the act. (The "entry" may only be the flash drive into a computer linked to the target system as the fifth column individual is probably a citizen in the country with security clearance.)

A third sort of malware is the Trojan Horse. Like the worm it is not self-replicating. It is not easily detectable at first and then attacks at a delayed interval. This weapon has the advantage of slipping under the firewall protection systems. However, it cannot be delivered to Intranet systems.

For the most part, these three sorts of malware will disable the operations of some computer driven facility within the country: electricity, sewage, water-treatment,

12 Aristotle, 1255a 20, ff.

13 See Geers, Dipert, Kelsey, and Harris.

14 Though this is generally the case, there are extenuating cases where sovereignty is breeched by attacks upon a surrogate —such as in the Bay of Tonkin (Vietnam War) or the USS Maine (Spanish-American War). However, the general pattern still holds.

15 Of course there have been many other instances in which civilians have been targets during warfare (such as biological and chemical agents), but the point here is that these instances violate traditional just war theory.

air traffic control, et al. For example in 2000 the Israelis disabled the public websites of Hezbollah and the Palestinian National Authority.[16] In 2001 because of a maritime dispute, China launched an attack against a California electric plant that almost caused the grid to shut down.[17] Though an egregious loss of property or life would constitute grounds for retaliatory war, the question still remains: what constitutes 'egregious'? Our assessment of this leads us back to the distinction between sabotage and an act of war mentioned at the beginning of this essay. The answer must take into account a cost/benefit assessment of outcomes. Our tolerance for damage caused by China would certainly be higher than that caused by a small country such as Grenada. Our grounds would be the same in each case, but the practical consequences of a retaliatory war against China are echelons higher than an attack on Grenada.

An interesting example of a coordinated cyber campaign was the launching of Duqu, Flame, and Stuxnet. The military objective was to: (a) obtain information on Iran's nuclear weapons program, and (b) to slow or disable said program. The program began with Duqu, a computer virus that was designed to copy the blueprints of Iran's nuclear program and to provide general information from a wide variety of sources that were infected as per the mission of viruses. Some believe that this attack was begun in Israel because the working hours of Duqu's operators corresponded with local time in Jerusalem (along with other cities in that time zone).[18] But this attribution has never been proven to everyone's satisfaction. Apparently, Duqu's mission was successfully achieved. It allowed the next step in the recognizance, Flame.

Flame was another virus that was launched in 2007. It was a reconnaissance tool to track the widespread activity of scientists and the operations of uranium enrichment centrifuges.[19] Again, because the malware attack was in the form of a virus, its effects were widespread. It was remarkable in its effectiveness because it delivered high yield information that gave an accurate picture not only of the activities of the scientists, engineers, and politicians involved in the project (personally), but also it described the activities of the centrifuge development and its ongoing operations. This virus went undetected for five years. The attribution is generally thought to be the United States, but nothing can convincingly be proven. In this case these two instances were examples of recognizance that is a stage in going to war.

Duqu and Flame set the stage for a response: the Stuxnet worm. In the case of the Stuxnet worm, the target was a nuclear power plant that intelligence (as per Duqu and Flame) said was being converted into a center to create nuclear grade material that could be used in a weapon. Iran had claimed that it only wanted to enrich uranium for use in power plants (a legitimate civilian use). However, that level of enrichment is only 3% to 5% The plant had enriched uranium over 20x—possibly on the way to the 80%-90% level necessary for a weapon.[20] The goal for Stuxnet was to disable the site and create havoc so that the deployment phase of enrichment was pushed back by three to five years. The actual result was a 24 month disruption. This attack worked effectively and involved no loss of life.

However, in other cases conventional warfare mixes with cyber warfare. In September 2007 the Israelis launched a cyber-attack against the radar and anti-aircraft devices in Syria. This maneuver aided the Israelis to successfully bomb a nuclear facility that also might have been on the verge of creating nuclear weapons.[21] Because Syria felt the cost of going to war with Israel to be excessive, there was no retaliation.

One can imagine that attacks upon air traffic control systems could also have the consequence of civilian aircraft crashes and the loss of life. Attacks on an electric grid[22] could have the consequence of stopping electricity to hospitals and causing deaths (assuming there is no comprehensive back-up system that is only available at a very select number of hospitals around the world). Or electric grid failures could severely disrupt fire, police, and other emergency personnel from being able to save lives and avoid domestic havoc. Food stores, sewage plants, water purification facilities would all be affected. What if there were a cyber-attack on the New York Stock Exchange? If the attack were sophisticated enough, bogus trades could be made and markets manipulated in such a way that the entire system would be at risk—and possibly not distinguishable from ordinary "legitimate" trades.[23] Since trading programs are so interconnected through programmed algorithms, it might be possible to create a crash (a one-day event until the automatic shut-off is activated) and then be subject to follow-up attacks. The stock exchanges have automatic systems for trading irregularities but are less well-prepared for cyber-

16 Hughes: 528.

17 Geers, 2008 & 2010.

18 Perlroth (2012).

19 Anonymous, *New York Times* (2012).

20 Anonymous, *New York Times* (2011).

21 Eshel: http://www.military.com/features/0,15240,210486,00.html. Accessed October 15, 2011.

22 Harris: 70.

23 Of course, Internet Security experts have long understood this problem. I was present at one such mock session at Marymount's graduate Computer Security Program. Though the technical details were beyond my ken, I was made keenly aware of how much damage might be irretrievably caused by a clever black hat attack.

attacks.[24] This could cause untold international economic havoc.

No matter the delivery device, attacks upon airports, electric grids, or stock markets could have wide-ranging effects that would blur the classic distinction between military and civilian (non-combatant) targets. This could be an instance of a stretch upon the traditional categories of just war.

Of course, a final telos for malware would be *espionage* (as per Duqu and Flame). Traditionally, espionage is not a cause for war. However, *spyware* is another popular form of malware. It is not the same as the destructive genus, but like the Trojan Horse, it tries to be undetectable and deliver important classified information for foreign intelligence agencies. Spyware can be employed as either a virus or a Trojan Horse. Since spyware is really very similar to other espionage strategies in times past, it does *not* offer a challenge to traditional just war theory.

Attribution and Target Distinction

One of the pivotal differences that cyber warfare poses from the traditional paradigm is attribution.[25] The question of "who did what to whom?" was generally easily answered when there were physical events of individuals crossing territorial lines and occupying land and strategic positions in the opposing country. However, when the battlefield is really fiber optic cable, phone lines, and cell phone relay stations, the place of interest is largely inscrutable. Privacy has long been a part of the architecture of the Internet. Messages generally begin on one relay network and then are routed through the most efficient set of relay networks until they reach their destination. Each relay network has identifiable origin and terminus points. These can be exploited by the black-hat hacker or cyber attacker to hide the identity of the perpetrator. For example, if Russia wanted to attack Estonia or Georgia, they could first send out a foray to Nigeria in Africa and then back to Estonia to make it appear that Nigeria was attacking them.[26] Without further protocols, what appears at first glance to be an attack by Nigeria against Estonia or Georgia could instigate a counter-attack (see below). This counter-attack would be mistaken because the real culprit (here assumed to be Russia) was not known and another innocent party was blamed. As the Internet has grown more ubiquitous, a careful rogue can literally make himself invisible.

A simple fix for this problem would be to change the Internet by creating an identification trail so that all traffic could always be tracked to its source. This would require international cooperation since if only one country went forward, counterfeiting would be easy. However, this would not solve the problem with the Stuxnet worm that was allegedly inserted into the closed computer system of Iran's main nuclear power facility. In this situation we have a sabotage situation not unlike the traditional blowing up of a bridge or other tangible target. (As mentioned earlier the extent of property damage or subsequent loss of human life would determine whether such aggressive actions constituted a ground for going to war.)

Without a new international protocol to change the architecture of the Internet (by requiring identification of all traffic) it is very possible that we will devolve into an attitude of continual war. This is because each major player will consider himself involved in *bellum omnium contra omnes* –a war of all against all.[27] This would be an unfortunate outcome because the various advances in cooperation—particularly in international commerce—would be set back and the plight of humankind would be more perilous.

Target distinction is another critical part of just war theory. In *ius in bello* rules, the warring factions may attack military targets or civilian/non-combatant targets that are enabling the military to fulfill its mission. However, because most infrastructure that might be attacked in cyber warfare is *dual use*, this distinction can become lame. For example, if the air traffic control system is deployed by a dual use GPS/radar system, the disabling of such a system for military use might also cause airplane crashes of civilian planes. (The same thing could also occur on rail traffic that is also a dual use system that is heavily computer driven.)

Or if the electric grid were the target, and it was dual use with military and civilian customers (such as hospitals), then an attack on the electric grid to harm the military might have considerable collateral damage on hospitals and operating theaters with the resultant loss of non-combatant human life.

Other cases involving water, sanitation, or communications facilities (that might also take out civilian police) could have considerable civilian casualties. This is due to the fact that there are so many dual use facilities in most countries in the world.

Territoriality and Neutrality

The next category relates to what we discussed in the last section. The traditional definition of war cites the territorial sovereignty of each nation. Since the Internet

24 Roberto Baldoni and Gregory Chockler eds. have set out analysis and strategies for financial market defenses. The editors claim that the major financial markets and other financial institutions are not well-prepared for a sophisticated cyber-attack.

25 Cowan: 25.

26 Though there were real attacks on Estonia and Georgia, this scenario is rather fanciful: see Dipert: 384.

27 This is also a concern of Hughes: 525.

goes through almost every nation on earth in some way (hard wired or broadband through the wireless air) and since there is no protocol for identification, the traffic on the Internet is largely anonymous (to anyone who wants to cover her trail), the traditional attachment to or infringement upon territoriality is difficult or impossible to determine. This would still be the case if the identification protocol mentioned above were adopted unless there were additional markers of data packets that went through virtual customs agents that would subject each packet to some sort of quick cyber check. Presumably, this might go part of the way toward maintaining territoriality. It is true that data packets could be disguised, but this would be analogous to those at border crossings who attempted entry under disguise (though the time involved would be much less—probably less than a second).

However, since the Internet has been built upon the admiration of speed and efficiency, even a second or so at each international boundary might add several seconds in the delivery of searches and downloading of messages and data. In our present climate, this would be seen practically as a large hurdle to clear.

With respect to just war theory, territoriality becomes important as it impinges upon the right to neutrality. The prime example of the exercise of the right of neutrality is Switzerland which was granted this right in 1815 under the Congress of Vienna. This right has been re-affirmed time and again internationally and most recently by the Treaty of Lisbon that came into effect in 2009.[28] If a country wishes to remain neutral, then it does not want to help either side in a war. Since the present architecture of the Internet does not allow for identification of *who* is sending *what* to *whom* maintaining the sovereignty of one's territory (physical optic cable) or one's air space (wireless broadband) is impossible under our current IT structure. In cyber warfare, everyone can be brought into the picture—even unwittingly. This reality leads to the unacceptable consequence of *bellum omnium contra omnes* — a war of all against all. Such an outcome would render the entire world to be in constant and perpetual war.

Attack and Response

The final category to be examined in this section is the difference this all makes. What if country X engages in a cyber-attack against country Y? What would the appropriate responses be? Consider the following:

1. Country X engages in a cyber-attack against country Y, and Y decides to engage in a counter cyber-attack against X.
2. Country X engages in a cyber-attack against country Y, and Y decides to engage in a conventional counter attack against X.

In situation one, the traditional just war theory is not in too bad of shape. The principle of proportionality would seem to be most relevant. If X's attack against Y cost $Z amount of money and no loss of human life, then a counter-response in the Z-range would be justified.[29] This, of course, assumes that the attribution issues have been resolved. (I believe that unless my suggestions are adopted, there will always be inaccuracy here—largely driven by prejudice and ethnocentrism.) If one does not know who did it, then how can one respond? Social prejudice may well rule the day, but that would be no better than a "lynching."[30] If we get the attribution wrong, then there is no proper defensive response, but instead another offensive act. The doomsday model of '*bellum omnium contra omnes*—a war of all against all' would be ever closer.

But what of option #2? This is more difficult because it involves goods of a different type. On the one hand we have an economic loss and on the other we have a response that will involve the loss of lives on both sides. Going into conventional war against another nation is no small event. How much economic disturbance would justify it? These sorts of calculations need to be made in an international forum: a new Geneva Convention.[31] If some foreign country were to shut down *Amazon.com*, would that be enough to respond with conventional war? What about disabling Hoover Dam? What about shutting down the power grid from Boston to Washington, DC? Where do we draw the line so that the general

28 http://ec.europa.eu/news/eu_explained/091201_en.htm. Accessed October 1, 2012.

29 Of course we must also view the real "cost" of an attack in the context of one country's ability to restore itself. For example a one billion dollar damage to the United States is far different than a one billion dollar damage to Haiti. The traditional criterion of *proportionality* can take this into account.

30 The manner in which prejudice is often the first response in times of uncertainty was demonstrated in the Mura Office Building bombing. In the days just after the attack, the public view was that it was an act of terrorism perpetrated by foreign Muslim extremists. This, of course, was wrong. It was a domestic terrorist with ties to non-denominational Christianity. The same dynamics occurred during the run-up to the Spanish American War after the publicity over the explosion and sinking of the U.S.S. Maine in Havana Harbor that killed almost three-quarters of the crew. Though the cause was unclear, the yellow journalism of the time using some underlying racist background assumptions stirred up public sentiment that led to war.

31 Perhaps the US National Research Council's 2009 report on cyber-attack would be a good starting point for a new international protocol.

intuition of proportionality is met? This is a gap in the present understanding of the base-line justification for conventional war in response to cyber-attack. This is not an insurmountable task, but at present the boundary conditions are not well-defined. It would be better if an international discussion were to take place in order to address these issues—perhaps involving the International Court of Justice and the World Trade Organization for adjudication of economic tort.

One way to move in this direction would be to come to some sort of agreement about historical attacks that resulted in loss of life and/or property that all agree were acts of war. These could be viewed as percentages of local or national economies. Up to this point, the acts would be viewed as sabotage and fines would be leveled against the offending country. Past the point, the action would be referred to the U.N. Security Council and to regional military pacts such as NATO.

New Ways to Think about War after Cyber Attacks

This essay has *not* suggested that the traditional categories of just war theory be jettisoned. Rather, what has been argued is that they need to be expanded to include the new dynamics of warfare that include recognition of cyber warfare (though other issues such as the overwhelming reality of intra-state warfare, non-state sponsored terrorism, and ever expanding robotic warfare should also be addressed).

1. Regarding cyber, warfare new rules must be drawn up. Rules governing *anything* only work when the participating parties agree to the rules and the mechanisms for enforcement. In my two years at the Center for American Progress (a Washington, D.C. public policy think tank) it became apparent to me that both of these proposals will not be easy to accomplish. The most useful suggestion that I would put forth that might bring this about is that in the case of cyber-warfare we should move away from the *at-fault liability* mindset that presently exists in just war theory to one of *strict liability*. This new mindset would look at the damage caused by some actor and move it into international civil law. This would permit monetary compensation based upon strict liability tort. The top 75 economies in the world have assets spread around the world in major G-6 countries that could be frozen should the fines not be readily paid.

2. Cyber-warfare requires a set of internationally recognized compensation categories for loss of property and life—though this can be contentious (as we found out when the United States tried to compensate the families of victims in the 9/11 attacks). To avoid this, monetary disbursement levels need to be established. These would be on the line that international insurance policies already adopt when creating their policies for large international players. This is especially important for errant attacks or unforeseen consequences.

3. A fifth Geneva Convention. The last four: 1864, 1906, 1929, and 1949 served their eras well, but issues raised in this essay (particularly the adoption of a civil compensation system) would allow for another source of counter-attack—not on the battlefield but in the courts of international justice. Among other updates one prominent area for new regulations concerns cyber warfare.[32]

Wouldn't it be a blessing in disguise if the contemporary challenges to the just war theory of international conflict actually resulted in a new mechanism (rooted in recognized law and backed up by the global banking system) that was actually able to find an original way to settle acts of aggression on the territory and sovereignty of another nation through recognized legal protocols instead of the shedding of blood in the traditional way or via cyber destruction?[33]

The integration of an updated rule of international law, that is enforceable, would bring just war theory up-to-date, and allow cyber warfare to be included within a revised cannon of just war theory. The world would be the better for it.

References

Anonymous (2011) "Stuxnet" http://www.topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html. Accessed October 15, 2011.

——— (2012) "Cyber Attacks on Iran: Stuxnet and Flame." http://www.topics.nytimes.com/top/reference/timestopics/subjects/computer_malware/stutnex/index.html. Accessed July 12, 2012.

Aristotle, 1957. *Politica.* Ed.. Sir David Ross. Oxford: Clarendon Press.

Aust, Stefan and Anthea Bell (2009) *Bader-Meinhof: The Inside Story of the R.A.F.* New York: Oxford University Press.

Austen, Ben (2011) "The Terminator Scenario" *Popular Science.* January: 60-93.

Bailey, Beth (2009) *America*'s *Army: Making the All-Volunteer Force.* Cambridge, MA: Harvard.

Baldoni, Roberto and Gregory Chockler eds.(2012) have set out analysis and strategies for financial market defenses in

32 I would also add regulations concerning robotic warfare at the same gathering.

33 Of course, these proposals will work best with the network outside the G-8 countries (the eight largest economies in the world). These countries have a history of ignoring rulings from the United Nations. The result with these nations will probably be handled diplomatically on a case-by-case basis. However, having an agreed upon structure will still help with these negotiations.

Collaborative Financial Infrastructure Protection: Tools, Abstraction, Middleware. (Dordrecht: Springer.

Boylan, Michael. 2011. *Morality and Global Justice: Justifications and Applications.* Boulder, CO: Westview.

——— 2004. *A Just Society.* Lanham, MD and Oxford.

Buzan, B. (2002) "Who May We Bomb?" in Ken Booth and Tim Dunne, eds. *Worlds in Collision: Terror and the Future of Global Order.* Basingstoke: Palgrave: 85-93.

Coady, C.A.J. (2004) "Terrorism and Innocence" *The Journal of Ethics.* 8.1: 37-58.

Committee on Offensive Information Warfare of the U.S. National Research Council (2009) http://www.icrc.org/web/eng/siteengo.nsf/iwplist163/d9dad4ee8533daefc1256b66005affef. Accessed October 29, 2011.

Cowan, Gerrard (2009) "Defending Against a New Kind of Warfare" *Jane*'s *Defence Weekly.* 46.27: 25.

Dipert, Randall R. (2010) "The Ethics of Cyberwarfare" *Journal of Military Ethics.* 9.4: 384-410.

Eshel, David (2010) "Israel adds Cyber-Attack to IDF" *Aviation Week*'s *DTI.* http://www.military.com/features/0,15240,210486,00.html. Accessed October 15, 2011.

Esposito, John L. (2011) "Arab Spring: changes and perspectives in transitioning from dictatorship to democracy" 20-October, 2011, public lecture Georgetown University.

Geers, Kenneth (2010) "The Challenge of Cyber Attack Deterrence" *Computer Law and Security Review.* 26: 298-303.

——— (2008) "Cyberspace and the Changing Nature of Warfare" *SC Magazine.* http://wwwscmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article115929/. Accessed October 15, 2011.

Harris, Shane (2010) "E-Warfare" *Wilson Quarterly.* 34.1: 69-70.

Hughes, Rex (2010) "A Treaty for Cyberspace" *International Affairs* 86: 523-541

Kelsey, Jeffrey, T. G. (2008) "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare" *Michigan Law Review.* 106: 1427-1451.

Killmister, Suzy (2008) "Remote Weaponry: The Ethical Implications" *Journal of Applied Philosophy.* 25.2: 121-133.

Krentz, Peter (2011) *The Battle of Marathon.* New Haven, CT: Yale University Press.

McMahan, Jeff (2004) "The Ethics of Killing in War" *Ethics* 114.4: 693-733.

Paden, John N. (2005) *Muslim Civic Cultures and Conflict Resolution. Washington, DC: Brookings Institution.*

Peace Reasearch Institute Oslo: PRIO,(2004). From Credo Reference, www.credoreference.com/entry.do?pp=1&id=84485.

Perlroth, Nocole (May 31, 2012) "Researchers find Clues in Malware" *New York Times:* B-1.

Pollini, Alessandoo (2009) "A Theoretical Perspective on Social Agency" *AI & Society.* 24.2: 165-171.

Primoratz, Igor (2002) "Michael Walzer's Just War Theory: Some Issues of Responsibility" *Ethical Theory and Moral Practice.* 5.2: 221-243.

——— (2005) "Hands Up Who Wants to Die?" *Ethical Theory and Moral Practice.* 8.3: 299-319.

Reichberg, Gregorty M., Henrik Syse, and Endre Begby (2006) *The Ethics of War: Classic and Contemporary Readings.* Oxford: Wiley-Blackwell.

Romm, James (2011) *Ghost on the Throne: The Death of Alexander the Great and the War for the Crown and Empire.* N.Y.: Knopf.

Simonite, Tom (2009) "Can We Trust Military Drones to Decide When to Fire?" *New Scientist.* 202.2713: 20.

Torrance, Steve (2008) "Ethics and Consciousness in Artificial Agents" *AI & Society.* 22.4: 495-521.

Walzer, Michael (1977) *Just and Unjust Wars.* New York: Basic Books.