CHAPTER

14

Ethics

INFORMATION IN THIS CHAPTER

- Ethics in Cyber Warfare
- Bellum Iustum—Just War Theory

Ethics is defined as "a system of accepted beliefs which control behavior, especially such a system based on morals [1]." Ethics is highly subjective, and can vary between cultures, businesses, or even individual upbringing. Many of the systems of ethics that are in place are of religious or cultural origin, and may present completely different concepts of what is right and what is wrong.

In the business world, we can see repeated failures of ethics in the form of one calamity after another being broadcast in the media. One of the more famous incidents is the Enron scandal of 2001, in which the company conspired to hide billions of dollars in debt from its shareholders and eventually went bankrupt [2]. The Sarbanes-Oxley Act of 2002 was passed in a large extent due to the Enron scandal, and actually specifies that corporations must publish a code of ethics for their senior officers, or disclose their reason for not having one [3].

When considering activities that might be classified as cyber warfare, we also need to consider the ethics of the situation. Cyber operations are a new dimension in warfare, and do not have all of the same attributes that traditional warfare does. We need to take into consideration that some of the items that may be very clear in conventional warfare such as deciding if we are really being attacked, who is attacking, whose infrastructure we are using to conduct the attack, who we are attacking, and that both the immediate and secondary consequences of such attacks, may not actually be as simple as they seem during planning.

Additionally, in cyber warfare, the right to go to ware, in both a legal and moral sense may be a line not as cleanly drawn as we find in conventional warfare. We may not only have problems distinguishing who our attackers are, but we may also have issues in limiting our response to those that we think are attacking. As networks are not necessarily geographically bounded, we may cause considerable collateral damage in the process of carrying out our operations.

http://dx.doi.org/10.1016/B978-0-12-416672-1.00014-3

We can see an example of a questionable basis to conduct cyber war activities in the hacktivist attacks that took place as a direct result of Julian Assange (of Wikileaks fame) being arrested in late 2010 [4]. A variety of attacks, many of them Denial of Service (DoS) oriented, were launched against organizations that were thought to have taken action against, or to not have supported, Wikileaks or Assange, with a few of the larger being Amazon, Mastercard, and PayPal.

ETHICS IN CYBER WARFARE

In cyber warfare, there are certain concepts that have the possibility to change the way that the laws of war are interpreted. When we look at cyber warfare-related issues we may diverge somewhat from the more clean-cut situations that we come across in conventional warfare. For instance, the question of whether cyber warfare attacks constitute use of force and the lack of clarity in attribution for such attacks are problems with no easy solution.

Use of Force

An excellent question, and one that commonly comes up during discussions of cyber warfare, is the question of the *use of force*. In conventional warfare, *use of force* is generally an obvious occurrence, accompanied by the arrival of troops, fighter jets overhead, and things exploding.

TIP

When talking about the legal authority to conduct warfare, cyber attacks are judged by their effects. The consequences of a cyber attack are considered to be generally equivalent to a kinetic attack producing the same results. If a cyber attack causes system outages in a hospital and results in a number of deaths, it may very well be considered to be a violation of the laws of war, and therefore possible a war crime.

In the *use of force* in conventional warfare, we might bomb a portion of our opponent's infrastructure in order to disrupt their electrical grid. In cyber warfare, *use of force* could mean the sabotage of a Supervisory Control and Data Acquisition (SCADA) or Industrial Control System (ICS) system controlling a portion of the electrical grid, and the subsequent failure of the grid. Although we might never have moved a single combatant, or, in fact, moved from our desk, we have still achieved our goal of disrupting the infrastructure of our opponent. This tends to imply that the term *use of force* is inadequate, or needs to be redefined, in order to include attacks of a cyber nature.

Although it has yet to be specifically quantified in a particular law, case law, or treaty, there is a common understanding regarding the qualification of a cyber attack as a *use of force*. In essence, if the cyber attack causes the equivalent amount of damage that would be rendered by a kinetic attack [5], i.e., a conventional warfare attack, then it would be considered an equivalent *use of force*. For example, if a cyber attack were used to cause an airliner to crash,

the attack would be considered the equivalent of a kinetic attack, such as shooting it down with a missile, causing the plane to crash.

As mentioned, the definition of *use of force* is still somewhat of a state of flux. More recently, the Tallinn Manual on the International Law Applicable to Cyber Warfare states "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" [6]. While this definition may sounds very similar overall, the Tallin Manual goes on to provide additional details on use of force, including "providing an organized group with malware and the training necessary to use it to carry out cyber attacks against other States" [6], would qualify as such.

Intent

When dealing with network, system, infrastructure, or other issues that are causing us a great deal of trouble, it is easy to imagine that they are the intended actions of a malicious attacker.

Given the broad arsenal available for cyber attacks, such an attack could look like a random occurrence; a service crashing, files being altered or deleted, unusual traffic to a particular port or ports, accounts being locked out repeatedly, or any number of similar problems.

Problematically, such problems can also be caused by any number of legitimate issues. Services may crash due to faulty operating system or application patches, files may be altered or deleted on accident by legitimate users, unusual traffic to ports may be due to application configuration issues, and accounts may be locked out repeatedly due to login attempts by maintenance processes. Any number of such issues may appear to be an attack and, without taking the time to determine the actual intent of the "attacker" we may jump to the wrong conclusion and take rash actions.

Attribution

Beyond intentionally obscuring the source of an attack, steps can be taken to cause the attack to be attributed to another source. Using another country or organization to mask the source of an attack can lead to tensions, or outright attacks on the systems behind which we are hiding, potentially drawing our unwitting shield into a conflict. Although such tactics are used in the intelligence world for exactly these purposes, they are not a component of outright warfare, and may be considered to be "bad form" by some parties.

Military Laws Based on Ethical Systems

When conducting warfare, in either a conventional or cyber sense, nation states, but not necessarily non-state actors, generally follow certain sets of rules in order to prevent truly horrific weapons from being used, civilians from being attacked, hospitals from being bombed, and other similar actions that are generally considered to be morally reprehensible. At present, this set of rules is known as the law of armed conflict, a set of laws and treaties with a basis in ancient Rome.

Law of Armed Conflict

The law of armed conflict, at present, comprises the Geneva Conventions, the Hague Conventions, and a number of other treaties and laws. These laws are considered to be binding for the countries that are signatories to the treaties of which they are composed [7], although it is important to note that not all countries are party to such treaties. The laws specify what countries are and are not permitted to do in times of war, as well as the applicability to those that are non-state actors and those that are not signatories to the treaties. The Hague Conventions are somewhat more focused on the actual conduct of war, while the Geneva Conventions are more oriented in a humanitarian direction.

There were two Hague Conventions, one in 1899 and one in 1907, both conducted at The Hague in the Netherlands [8]. The first Hague Convention produced four major sections and three declarations related to the general conduct of war and the use of projectiles. The second Hague Convention, consisting of thirteen sections, established voluntary arbitration, set conventions on the collection of debts, expanded upon the rules of war, and laid out the rights and obligations of neutral parties.

The Geneva Conventions are composed of four conventions and three protocols, developed between 1864 and 1949 [9] and are the standards in international law for the humanitarian treatment of victims of war. These conventions cover the treatment of the sick and wounded, prisoners of war, civilians, and medical and religious personnel.

The law of armed conflict was developed in an attempt to mitigate the atrocities of war. It was also developed to deal with issues of warfare that take place on an entirely mental and physical level. Since we have added cyber warfare as an additional dimension, we need to either adapt or reinterpret the existing laws of war to fit, or create new laws to fit some of the special situations that cyber warfare creates, as we discussed earlier in this chapter in the section on the ethics of cyber warfare.

It is also important to note that the law of armed conflict is primarily intended to govern the conduct of war between states. In cyber warfare, it is entirely possible that we will find ourselves facing an opponent that is fully capable of carrying out attacks that would be considered an act of war if launched by a state, but are in fact sourced to an individual or a small group. This situation is specifically covered in the following section on *jus ad bellum*.

When we look into the specifics of the laws of warfare, we find that they are constructed on an older set of concepts called *bellum iustum*, or just war theory.

BELLUM IUSTUM (JUST WAR THEORY)

Just war theory gives us a good framework on which to discuss the ethics of warfare in general and more specifically, of cyber warfare. In just war theory, we look at conduct during three different phases of warfare; beginning a war (*jus ad bellum*; the right to wage war), during a war (*jus in bello*; conduct during war), and ending a war (*jus post bellum*; ending a war).

When discussing just war theory, the right to wage war, and the proper conduct during war, are universally included. These principles find their origin in ancient Rome, often first attributed to Cicero, and have been the basis of the rules of warfare from then into modern

FIGURE 14.1 Immanuel Kant, from the painting by Döbler.

times. Justice after war is a newer concept, and has its basis with Immanuel Kant in the eighteenth century [10] (shown in Figure 14.1) [11].

Each major section of *just war theory*, *jus ad bellum*, *jus in bello*, and *jus post bellum*, contains a number of principles that provide more specific guidance. As some of these principles have been modified, removed, added, and argued over for thousands of years, the specific principles and their meaning vary greatly from one source to another. With sufficient research, it is possible to find two entirely different sets of principles for a given concept, but the general ideas remain the same for each.

Jus ad Bellum (The Right to Wage War)

Jus ad bellum discusses the right to wage war. The five principles of *jus ad bellum* are: right authority, right intention, probability of success, last resort, and proportionality [12]. The right to wage war is a concept that is largely tied to states, which are much more bound to the laws of war than individuals or organizations, criminal or otherwise. In the case of such non-state attackers, the concept of the right to wage war may be reduced to more of a question of having the capability to do so. For those who have no intention of obeying domestic or

international laws in the first place, the legal and moral barriers posed by the laws of warfare are likely no impediment at all.

Right Authority

The legal authority that allows us to carry out attacks comes from a combination of laws, on a national and international level, treaties, and various other institutions. How exactly such laws relate to issues of cyber warfare is still in the process of being worked out and could definitely be an issue. We discussed this at length in Chapter 13.

Of particular note for applicability in cyber warfare is the fact that only the legitimate authorities of a state have the legal authority to wage warfare. In effect, this means that a state, generally the equivalent of a country, is the only entity that can legally wage war. For conventional warfare, the legal authority to wage war, on an international scale, and the capability to do so, generally match up fairly closely.

When we look at cyber warfare, the capability to conduct warfare differs greatly in the sense of resources required. A trip to a local computer store and a small amount of coding ability can be sufficient to arm a group or individual for cyber war. In such cases, the laws of war may not apply to criminal organizations, hacktivists, individual hackers, and the like, as they may be considered unlawful combatants. Unlawful combatants do not enjoy the protections of the laws of war and can be prosecuted under the laws of the state in which they are detained. Similar laws apply to corporations that conduct such unlawful cyber operations, although the consequences to them may be somewhat different from a legal standpoint.

NOTE

The laws that govern cyber crime and attacks vary quite a bit from one country to the next. Certain countries with laws that are more lax on such points, Bolivia for instance [13], can provide a good home, or at least a good place for collocating servers, for those non-state actors that conduct cyber attacks. As they are not bound by the laws of war, this can provide them with a certain measure of safety from a legal perspective.

In order for a non-state actor to be detained or prosecuted as an unlawful combatant, they would need to have committed an act that would be considered to be a *use of force* if they had been a nation state. If we look back to our discussion on the *use of force* earlier in this chapter, the common understanding is that, at present, *use of force* in cyber attacks is decided by the results of the attack. Unlike conventional warfare, a cyber operation of sufficient effect to be classified as *use of force* can very easily be carried out by an individual or small group.

Right Intention

Right intention in warfare specifies that we may only use or threaten force against another state for a truly just cause. It is understood by the signatories to the United Nations (UN) Charter that this specifically refers to a response to the *use of force*, and not other actions of an unfriendly nature, such as "unfavorable trade decisions, space-based surveillance, boycotts, severance of diplomatic relations, denial of communications, espionage, economic competition or sanctions, and economic and political coercion [5]," regardless of the way in which such attacks are used. Such unfriendly acts would include many attacks of a cyber nature,

excluding an attack that had an effect qualifying it as a *use of force*. While these may not be classified as actual acts of war, the results can still be devastating.

Probability of Success

The principle of probability of success dictates that force may not be used in a futile war effort. As we have already discussed, the distinction between what does and does not constitute *use of force* depends on the ultimate effect of the action in question. In the case where a cyber attack did not result in an outcome of a physical nature, it would likely not be considered a *use of force*. This leaves the possibility of a state using lesser attacks that are of a harassing or disruptive nature without violating this particular tenant of jus ad bellum. It does seem likely that the definition of use of force will need to be changed at some point, specifically to avoid parties using this as a loophole through which to conduct cyber attacks with impunity.

Last Resort

The principle of last resort stipulates that force may be used only after diplomacy fails, or is considered to not be practical. As is the case in the principle of probability of success, the definition of *use of force* in cyber warfare is an issue of importance. Although the actual issue of *use of force* might be problematic, there are many cyber attacks that could be used short of the *use of force*. In the case of attacks that do equate to *use of force*, for UN signatories, approval by the UN Security Council would likely be required in most cases [5].

Proportionality

The principle of proportionality states that the benefits of warfare must outweigh the harms that are caused by it. In cyber warfare, due to the potential unpredictable results of our attacks, judging proportionality may be a somewhat difficult prospect. While we can launch a cyber attack with the intent and relative surety that it will have a limited set of effects, the possibility always exists that we will do a far greater amount of harm than was originally planned.

Jus in Bello (Proper Conduct in War)

The idea of *jus in bello* specifies how a state must act in times of war. The two principles of jus in bello are distinction and proportionality [14]. Distinction covers the way that we carry out the war itself, in the sense of which targets are and are not legitimate. The concept of proportionality means that we cannot attack a legitimate target and cause a great deal of collateral damage in the surrounding area without cause to do so.

Distinction

The concept of distinction specifies that war should not be directed at noncombatants and neutral parties. In conventional warfare, while this concept is not always easy to carry out, it is rather clear-cut; we should not attack civilian targets without affecting a sufficiently valuable military goal as the end goal. In the logical world, where cyber operations are carried out, this distinction is more difficult to make, due to the intermingled nature of military and civilian networks and systems. When we attempt to make the distinction between such targets, there may actually not be a separation, as many such targets will be dual use.

We also have some difficulty when it comes to the matter of neutral parties in cyber warfare. Given the nature of cyber operations, attack traffic can traverse a wide variety of networks and systems in order to reach its intended target. We may be routing packets through the networks of multiple different countries, some of them neutral, some of them not; and many of them completely unaware that the traffic is even going through their infrastructure. We also have the possibility of a target not actually being located in the state that is being attacked. Our opponent could have systems located in a multiple different geographical locations in order to render such systems more difficult to attack physically, and such a system might be physically located in a neutral country. This also brings up the question of whether there are obligations for a neutral party to take steps to stop attacks coming from or routing through their country. Such questions will likely not be resolved until sufficient cyber incidents have occurred that new laws are created to deal with them, or the present ones are given new interpretations to include them.

Noncombatants

Noncombatants are a particular issue in cyber war. In conventional warfare, the issue of not attacking noncombatants is somewhat clear-cut. In general, we do not want to bomb orphanages, hospitals, and other similar areas that are considered to be of a non-military nature. Although such rules do not always hold true, accidental strikes do happen and opponents do sometimes use such facilities as shields, but the rules are relatively clear.

When considering a cyber operation, the boundaries between what is acceptable and not acceptable are not as clear. At present, such activities are carried out almost universally over public networks, as these same networks are used by civilians and military equally. We cannot presently attack one group without affecting the other in an equal measure. When we destroy infrastructure in order to remove the capability for communications and propaganda from the hands of our opponents, we also disable such services for the civilian and noncombatant populace.

While it is easy to say that we cause no true or permanent harm by taking out the Internet connectivity in an area, we may be causing more of a significant impact than we might think. We may be disabling connectivity for those working for companies from remote locations, people who operate stores over the Internet, or schools that access educational materials online. Worse yet, we may be disabling the systems that enable the distribution of food and supplies, SCADA systems that monitor and control utilities, and other critical components. Removing the ability to run heating or air conditioning systems at certain times of year may indeed result in loss of life.

Destroying or disabling network systems or infrastructure in an area of poorer economic status may leave a considerable barrier toward the local populace being able to restore such functionality within any reasonable amount of time. Permanently removing such systems may have a profound effect indeed, even without shedding a drop of blood with the weapons of conventional warfare.

Proportionality

The concept of proportionality covers the effects of the attack in relation to the type of target being attacked. If we attack a target that is a military objective, we cannot cause harm

to targets that are civilian, noncombatants, or neutral parties while carrying out this attack that is in excess of the value of the original target.

Problematically, the effects of cyber attacks can be difficult to detect or quantify. Whether such attacks do physical damage or not, the estimated amount of damage done would need to come from the party being attacked, without any direct way of verifying such a claim by the attacker or any interested third parties. Since, other than any obvious physical components to the attack, there is no immediately and publically visible effect, such estimates can prove to be guesswork at best.

Additionally, some cyber attacks are reversible, and some are not. If we use something along the lines of a DoS or Distributed Denial of Service (DDoS) attack, the first order effects should be relatively reversible. When we stop the attack, a few systems may need to be rebooted or restored, but this should largely be the extent of any material damage. If we use a cyber attack to take control of the systems managing the water level in a dam and the dam breaches, then we have caused a great deal of physical damage that cannot be undone.

Collateral Damage

As with conventional warfare, we need to be concerned with our cyber attacks affecting people and facilities that are not considered to be part of the conflict. Considering that the systems and networks that provide the basis for such operations are the same systems and networks that public services operate over, achieving this separation can be rather difficult.

Given the present structuring of our networks, being able to direct our attacks so as to avoid impacting noncombatants, as is specified in the Hague and Geneva conventions that we discussed earlier in this chapter, may be very difficult, if possible at all. In the future, we may see changes to systems and networks in order to separate civilian networks from military networks in order to make such distinctions easier to arrive at in times of war or crisis.

Limiting Attacks

When we look at attempting to limit attacks in cyber warfare, we encounter a rather technically difficult proposition. As the Internet is not geographically bounded, attacks of a logical nature, even when carried out with the greatest care and planning, are very likely to have impacts that we do not anticipate.

WARNING

In the context of using malware as a tool of cyber warfare, limiting such attacks may prove to be very difficult indeed. We can certainly implement features in such tools in an attempt to limit them to a particular network, geographical area, or any of a number of factors, but such efforts will not always be successful. Even if we were to code our attack tools in such a way as to be limited to a particular IP address range, in order to only target a given organization, we would also be likely to infect geographically distant machines that were connected over Virtual Private Network (VPN) connections, and other similar cases. In effect, we would very likely spread a tool of cyber warfare into personally owned systems, other countries, and support organizations in very short order.

One potential solution to such issues is the implementation of logical borders to match our physical borders. In areas that are largely physically separate from other land masses,

Australia for instance, such an implementation may be somewhat easier to carry out, at least from a wired perspective. If we were to attempt the same in one of the countries in Western Europe, the task becomes considerably more difficult. Although challenging to implement, such divisions may be beneficial in the near future.

Jus Post Bellum (Justice After War)

Jus post bellum defines justice after war; basically how to properly shut down and handle the aftermath of the war. The principles of jus post bellum are: seek a lasting peace, hold morally culpable individuals accountable, and extract reparations [15].

Seek a Lasting Peace

As we discussed earlier in the chapter in the section on *jus ad bellum* when we covered the need for a legitimate authority for a state to wage war, peace must also be offered and accepted by a legitimate authority. While this is the normal state in conventional warfare, in cyber warfare, our opponent may very well be a non-state actor such as a hacker, hacktivist, criminal, or a corporation. In such a case, these non-state actors are likely to be considered an unlawful combatant.

Hold Morally Culpable Individuals Accountable

Holding morally culpable individuals accountable for actions under cyber warfare may be a difficult prospect. As we have discussed several times in this chapter, many cyber operations fall outside of the bounds of the *use of force*. For such activities, it is unlikely that there will be anything substantial for which someone might be held to account. For attacks that do qualify as *use of force*, finding a specific individual upon which to pin responsibility might be difficult.

For example, in the case where a malware infection caused the system responsible for formulating a particular medication to produce an improperly mixed batch, we have several points at which we could assign blame. We could blame the author of the malware, although proving that they had this particular intent in mind when writing it would likely prove difficult, if we could identify them at all. We could blame the worker at the facility that carried the malware in on a thumb drive and infected the system, although this was likely done completely by accident. We could blame the system administrator for not having sufficient controls in place to catch the malware, and so on.

In some cases, we may have sufficient evidence to attribute such attacks to individuals, if they indeed were attacks at all, but these are likely to be few and far between. Even in such cases, the possibility of being able to prosecute such actions will, in all probability, be limited to state-sponsored activities.

Extract Reparations

The process of extracting reparations for an act of war runs into many of the same difficulties that we find in attempting to hold individuals accountable for such actions. We may be able to link a cyber attack to a particular individual or state, but outside of an officially declared war, reparations seem unlikely. As is the case in many interactions that take place

in the world of the logical, attacks of a cyber nature will probably be of a less forthright and formal nature than conventional warfare.

SUMMARY

In this chapter, we discussed the ethical issue surrounding cyber warfare. Such issues differ significantly from those in conventional warfare due to the potential for cyber attacks to be misattributed. We discussed attacking ethically in cyber war, including issues such as secrecy in attacks, noncombatant immunity, and what constitutes use of force in cyber warfare.

We covered issues that may arise to the determination or improper determination regarding the specifics of an attack. It is entirely possible that due to configuration issues, hardware problems, application misbehaviors, or any number of other issues, that we might mistake a technical problem for an attack. There is also the matter of the intent behind the attack. Attacks may be malicious in nature, intended to draw attention, legitimate security testing, or prompted by any of a variety of other motivations. Being able to respond appropriately to the intent of the attack is important.

Just war theory provided us with a good framework in which to discuss certain aspects of cyber warfare. We covered the authority under which we conduct such operations, from both a legal and moral standpoint. We also talked about proper conduct during war, including properly proportional responses to attack, the legitimacy of attack and response, and the international laws of war, including the Geneva and Hague conventions.

Lastly, we covered collateral damage issues as relates to cyber warfare. We went over problems of limiting attacks in the virtual world, and the technical issues involved in trying to do so. Due to the intermingled nature of governmental and civilian networks, it may not always be possible to restrict our attacks to targets of a military nature. Despite taking steps to confine our attacks to certain areas, we may become the target of a great deal of public frustration due to the impact on non-military targets.

References

[1] Cambridge Advanced Learner's Dictionary. Definition of ethic noun from Cambridge dictionary online. Cambridge dictionary online, http://dictionary.cambridge.org/ictionary/british/ethic?q=ethic; 2013 [accessed 03.03.13].
[2] BBC News. Enron scandal at-a-glance. BBC News, http://news.bbc.co.uk/2/hi/business/1780075.stm; 2002 [accessed 03.03.13].
[3] Competence Software. Section 406 – Code of ethics for senior financial officers. Sarbanes Oxley simplified, http://www.sarbanesoxleysimplified.com/sarbox/compact/htmlact/sec406.html; 2013 [accessed 03.03.13].
[4] Vinograd C. Julian Assange arrested: Wikileaks founder taken into custody in London on Swedish warrant. The Huffington Post, http://www.huffingtonpost.com/2010/12/07/julian-assange-arrested-w_n_792956.html; 2010 [accessed 03.03.13].
[5] Owens WA, Dam KW, Lin HS. Technology, policy, law, and ethics regarding U.S. acquisition and use of cyber attack capabilities. Washington, DC: National Academies Press; 2009.
[6] Schmitt M. Tallinn manual on the international law applicable to cyber warfare. New York: Cambridge University Press; 2013.
[7] Solis G. The law of armed conflict: international humanitarian law in war. New York: Cambridge University Press; 2010.

[8] Yale Law School. The laws of war. Avalon project, http://avalon.law.yale.edu/subject_menus/lawwar.asp; 2008 [accessed 03.03.13].
[9] International Committee of the Red Cross. International humanitarian law – treaties and documents. International committee of the Red Cross, http://www.icrc.org/ihl.nsf/INTRO?OpenView; 2005 [accessed 03.03.13].
[10] Orend B. War and international justice: a Kantian perspective. Waterloo, ON: Wilfrid Laurier University Press; 2000.
[11] Anonymous. The project Gutenberg EBook of picturesque Germany, http://www.gutenberg.org/files/23446/23446-h/23446-h.htm; 2007.
[12] Maiese M. Jus ad Bellum. Beyond intractability, http://www.beyondintractability.org/essay/jus_ad_bellum/; 2003 [accessed 03.03.13].
[13] Lovet G. out-law.com. How cybercrime operations work – and why they make money, http://www.out-law.com/default.aspx?page=7791; 2007 [accessed 03.03.13].
[14] Moseley A. Just war theory. Internet encyclopedia of philosophy, http://www.iep.utm.edu/justwar/; 2009 [accessed 03.03.13].
[15] Dimeglio RP. The evolution of the just war tradition: defining Jus Post Bellum. Military law review, http://www.citadel.edu/smll/Seminar/Additional%20Resources/DiMeglio,%20The%20Evolution%20of%20the%20Just%20War%20Tradition,%20Military%20Law%20Review,%20Winter%202005.pdf; 2005.