ASIAN
HORIZONS
Vol. 10, No. 1, March 2016
Pages: 69-84

CYBERWAR IN CATHOLIC ETHICS

Wojciech Morański[♦]
Boston College

Abstract

The reality of cyber warfare becomes frequently more present in public debate. That relatively new phenomenon creates a space for new kinds of abuses that might have disastrous effects on the wellbeing of the whole society. This paper argues that the Catholic Church's achievement in the domain of social ethics can bring interesting contributions to these studies. In the first section a study of the nature of cyberwar is presented, some examples of cyber attacks and international reactions to that threat are given. In the second section two examples of ethical approaches to cyberwar by lay authors are given in order to present the actual possible directions for investigation in the ethics of cyberwar. In the third section two documents published by the Catholic Church are studied. Neither of those two documents speaks directly about cyberwar, therefore author's own application of them to this new reality is presented.

Keywords: Cyberwar, Cyberwarfare, Stuxnet, Ethics, Catholic Social Teaching, Ethics of Internet

1. What is Cyberwar?

Modern societies depend on digital networks and that reliance grows all the time. The network has become a daily companion for many people. For plenty of them it is their place of work or business. National security depends on the Internet as well. Modern installations, both military and civil, communicate automatically

[♦] **Wojciech Morański, SJ** obtained his Master's in Computer Science from the University of Science and Technology (AGH) in Kraków, Poland, a Bachelor's of Philosophy from Jesuit University Ignatianum in Kraków, Poland, and a Bachelor's of Theology from Comillas Pontifical University in Madrid, Spain. He is currently working toward a Licentiate in Sacred Theology at Boston College, USA. His research is centred on ethics in the digital society. Email: wmoranski@gmail.com through the network. Therefore, all the vulnerabilities of the network are a threat for society's wellbeing.

There are plenty of methods that can disrupt network operations. *Encyclopaedia Britannica* defines three layers on which the network operates and which may be attacked.[1] The first is the physical layer that includes all hardware equipment such as computers, cables, routers, satellites, and others. That layer may be attacked by physical destruction or disruption, for example by electromagnetic interferences. The second layer is the syntactic layer that consists of software that controls the information flow in the physical network. That layer includes operating systems, protocols, application programs and others. That layer is normally attacked by malware software such as viruses, worms, exploits, rootkits, and others. The third layer is the semantic layer that includes human processing of provided information and interaction with the system. That layer is especially vulnerable to phishing, baiting, and other social-engineering techniques. There are attacks that use two or all three of those layers. For example the spreading of the Stuxnet worm was probably introduced into the system by direct human action, propagated thanks to holes in the operating system, and finally affected the operation of the physical machines. It shows how to design an integrated and multilayer operation in cyberspace.

Encyclopaedia Britannica defines cyberwar as "war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states."[2] This means that cyberwar is always an inter-state event. That excludes acts of cyber espionage, cyber terrorism, and other forms of cybercrimes from the strict definition of cyberwar. Moreover, it is very difficult to prove that a particular cyber attack is indeed an act of cyberwar because of the two following facts.

Firstly, tools and methods needed to perform a cyber attack are much cheaper than any traditional weapon. The skills and resources needed to deploy such an attack are easily achievable by the network itself. It makes a cyber-weapon potentially accessible for everybody who is connected to the Internet. Therefore, it is very difficult to distinguish if a particular strike is conducted by the government, by some secret army of hackers or simply by skilled civilians, without

[1] Britannica Academic, "Cyberwar," accessed December 11, 2015, http://academic.eb.com.proxy.bc.edu/EBchecked/topic/1498241/cyberwar.

[2] Britannica Academic, "Cyberwar."

any relation to state structures. The Geneva Convention does not define in a clear way the case of an attack organized by civilians. Probably, an attack led by a group of civilians would rather be cyber terrorism than cyberwar.

The second characteristic of cyber-conflicts is the anonymity of the network users. It is relatively easy to access the network without any previous identification. Moreover, there are easy-to-use methods to conceal one's identity. This might be done by physical connection to a public access point, by specialized software like The Tor network or by other methods. That makes it very difficult to determine the identity, location and motive of an attacker, and impedes a proper defence. It also makes possible a wrong accusation or even reprisal on an innocent country. Moreover, there are arising some transnational movements that claim to fight in cyberspace in the name of ideas that they defend. For example, one of the most frequently cited in mass media is the hacktivists group Anonymous. They usually proclaim cyber attack ahead of time and frequently are able to succeed it against national, social, political or even religious organizations.[3] However, their identity structure, supporters, motives and localization are hidden. Therefore it is difficult to acknowledge if that kind of activity should be treated as an international act of war.

Despite these difficulties, there are some examples of operations that fulfil the definition of cyberwar. Probably the most sophisticated technology was the Stuxnet, a computer worm. The program was discovered in 2010 but was circulating on the Internet at least from mid-2009. The operation was deployed in secrecy but from the beginning the United States and Israel were suspected to be behind it. In 2012 *The New York Times* confirmed that suspicion.[4]

The worm was programmed to strike only on very specific machinery manufactured by a German company, Siemens AG, used in nuclear power plants in Iran. Specifically, the worm was

[3] Katie Rogers, "Anonymous Hackers Fight ISIS but Reactions Are Mixed," *The New York Times*, November 25, 2015, http://www.nytimes.com/2015/11/26/world/europe/anonymous-hackers-fight-isis-but-reactions-are-mixed.html; Nicole Perlroth and John Markoff, "Attack on Vatican Web Site Offers View of Hacker Group's Tactics," *The New York Times*, February 26, 2012, http://www.nytimes.com/2012/02/27/technology/attack-on-vatican-web-site-offers-view-of-hacker-groups-tactics.html

[4] David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

reprogramming frequency-converter drives, causing a very high speed for the motors of centrifuges for separating nuclear material, and damaging those machines. The operation was efficient. By the end of 2010 approximately 100,000 computers were infected, and more than 60 percent of them were located in Iran. Experts estimate that Stuxnet broke about 20 percent of Iran's nuclear centrifuges and caused delay to, if not totally destroyed, Iran's ability to build nuclear weapons.[5] The effectiveness of that software, its precision in aiming at a target, and its very sophisticated technology proves that it was a well-designed cyber-weapon.

Naturally, the Stuxnet operation was not the only known cyber warfare act. There are other examples that have been classified as cyberwar even if they did not fulfil completely its definition. One of those examples is a three-week massive cyber attack on Estonia probably caused by Russian hackers in 2007.[6] During the operation multiple webpages belonging to the public institutions such as banks, newspapers, companies, government ministries, political parties, and others were blocked. The operation was taken as a form of revenge after the removal of the Russian war memorial from the city centre of Tallinn. In other words, the cyber attack had an international and political background. In reaction to that massive cyber attack NATO established a new Center of Excellence on Cyber Defense in Tallinn in 2008.[7]

That reaction of NATO was one of many acts of cyber counterintelligence. In the United States both the U.S. Airforce and the U.S. Navy have special units to perform military cyber-operations. In 2009 in the United Kingdom and in France special centres for cyber-security were established.[8] Probably other countries dispose of some type of military cyber-units but their existence may be not public.

Moreover, some diplomatic efforts have been undertaken in order to establish international rules for cyberspace. For instance, in

[5] William J. Broad John Markoff and David E. Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel," *The New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

[6] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007, sec. World news, http://www.theguardian.com/world/2007/may/17/topstories3.russia

[7] "NATO News: NATO Opens New Centre of Excellence on Cyber Defence," May 14, 2008, http://www.nato.int/docu/update/2008/05-may/e0514a.html

[8] Britannica Academic, "Cyberwar."

September 2015, during the visit of President Xi Jinping of Chinato the United States, cyber security was one of the main topics. At the end of the visit, President Obama said that, they reached a "common understanding" that state-sponsored cyber-intrusion is unacceptable and they will together seek "international rules of the road for appropriate conduct in cyberspace."[9]

In conclusion, the phenomenon of cyberwar is present in our world. The definition of this term, even if it is easy to express, is not easy to fulfil. There are some characteristics of the activity in cyberspace, like easy access, cheap tools and instruments, anonymous identity, location and motive of cyber-attackers that hinder a certain attribution of the term "cyberwar" to a particular cyber attack. Nonetheless, there are examples of cyberwar acts as well as national and international reaction on these events. Moreover, cyberwar become an important topic of international diplomacy. Therefore, a question arises about the proper ethical approach to that new phenomenon.

2. Ethical Approach to the Cyberwar

The common threat generated by the presence of cyber-violence caused a development of ethics related to that phenomenon. Since cyber-warfare is a complex reality, there are plenty of possible approaches. I present two different examples of the ethics of cyberwar that however come to very similar conclusions.

Is cyberwar a war? Larry May, a professor of philosophy, Law and Political Science, at Vanderbilt University, in his article "The Nature of War and the Idea of Cyberwar" argues that cyberwar does not fit to the definition of war, and calling it war has an ethically negative effect. In the beginning May presents a study of definitions of war since the 17th century, and their possible application to cyberwar.[10] He opines that the most accurate is the definition of Samuel Pufendorf which claims that war is "a state of men who are naturally inflicting or repelling injuries or are striving to extort by force what is due to them."[11] Hence, May claims that war defines a relation between two

[9] Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *The New York Times*, September 25, 2015, http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html

[10] Larry May, "The Nature of War and the Idea of 'Cyberwar,'" in *Cyber War: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein, Oxford: Oxford University Press, 2015, 3–6.

[11] Larry May, "The Nature of War and the Idea of 'Cyberwar,'" 6.

states which includes a use of violent force primarily directed at enemy soldiers. Thus, that definition is hardly applicable to cyberwar.

First of all, the main aim of cyberwar is to destroy some property such as computer programs, machines, connections, power supplies, etc. Even if it might harm or kill somebody, that would be a secondary effect and not the primary goal of cyberwar. Moreover, the recognition of the state of war involves an application of special rules and laws that do not restrict intentional wounding and killing of enemies. A war is never a good solution, but in some circumstances may be considered as a necessary evil, especially considering self-defence. For that occasion special criteria were developed in order to make war as humanitarian as possible. Nonetheless, large scale killing and wounding is still permitted. In the case of cyberwar, the large scale killing and wounding is neither present nor necessary. It is possible to wound or even kill enemy soldiers or civilians through cyber-weapons, but that is rather an accidental characteristic of cyber attacks, where essential component is destruction of an enemy's property. Moreover, the violation of territorial integrity of the state in the case of cyberwar is not clear. The cyber-operation on the enemy's territory normally does not include the presence of any troops. Therefore, in May's opinion, the application of laws of war to cyber-operations makes little sense.[12]

He claims that cyberwar have more in common with embargo, a term that belongs to the domain of economy. Embargos do not include any violation of territorial integrity of the country at which they are directed. Although embargos are focused on a destruction or limitation of access to some goods, and may cause great disruption and even deaths in the attacked country, still the rules of war normally are not applied to them. This means, that in the situation of embargo, reciprocal deadly aggression is still prohibited by law.[13]

That approach, in May's opinion, may limit cyber-weapon development. If the cyberwar is indeed a war it should be handled by the Department of Defence, specialized in development of arms. On the contrary, if the cyber attack is considered as an act of embargo it will be managed by the Department of State, where diplomacy is the primary tool rather than military operations. Another argument against treating cyberwar as war is an expected reaction of

[12] Larry May, "The Nature of War and the Idea of 'Cyberwar,'" 7.

[13] Larry May, "The Nature of War and the Idea of 'Cyberwar,'" 8-9.

undeveloped countries on a cyber attack. If it is an act of war it could lead those countries to respond with military aggression rather than to search for some diplomatic ways to find the solution.[14]

All those arguments lead May to the conclusion that cyberwar should not be considered as an act of war. Turning cyber-conflicts into the domain of economy and diplomacy may avoid an escalation of violence, a race of cyber-weapon development, and have a positive impact on international peace.

On the other hand, James L Cook, a professor of philosophy at US Air Academy, in his article "Is There Anything Morally Special about Cyberwar?" claims that cyberwar may be considered under the conditions of the Just War Theory (JWT). However, in his opinion, cyber-conflicts are morally special.

In the beginning, he notes that cyberspace is only a mean to perform an attack. The JWT says relatively little about means, focusing more on intentions and effects of the conflict. Therefore, its application to cyberwar should not be difficult as long as we can easily identify agents, their motives and effects.[15]

Nonetheless, those conditions are difficult to achieve because of three following characteristics of the network: ubiquity, uncontrollability, and what Cook calls neo-reality. Those characteristics in Cook's opinion make cyberwar ethically special but the application of JWT is still possible.

The cyberspace is very attractive territory for an ordinary user. At the same time that magical reality is little understood and is frequently treated as a kind of mystery. Its ubiquity refers to that mysterious perception of the network, which on the one hand, usually overestimates the possibilities in cyberspace, but, on the other hand, magnifies the fear about its possible danger. For example, it is a quite common tendency among average computer users to attribute any problems with the technology to some unknown virus or hacker. That fear, which normally is not rational, can violate perception of the true reality. It is especially dangerous for those who are responsible for security of the state. They are able to make impropriate decisions or undertake disproportional means as a reaction to that fear. For example, in November 2011, some unknown Russian hackers were

[14] Larry May, "The Nature of War and the Idea of 'Cyberwar.'"

[15] James L Cook, "Is There Anything Morally Special about Cyberwar?," in *Cyber War: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein, Oxford: Oxford University Press, 2015, 19–21.

erroneously accused of the destruction of the water pump at an Illinois utility. The computer inspection found a successful login to the pump's system from the territory of the Russian Federation. That discovery was a sufficient argument to raise a cyber-terrorism alert. Later investigation showed that the authorized technician, who was then on his holidays in Russia, was asked to do some small online inspection. That action had no relation with later damage of the pump, but caused the avalanche of events.[16]

The uncontrollability refers to the apparently independent multiplication and propagation of pieces of information, ideas or memes.[17] The spread of memes may be dangerous and may even harm physically other humans, for example in the case of propagation of powerful ideologies. The network makes that propagation much stronger and less predictable because it does not need any human intermediary, nor does the recipient need to be a human person. The meme can find its way directly from the creator to the recipient and cause some action, including a kinetic one. Moreover, the meme might have some level of independence, as is the case with computer viruses or worms. Therefore, for many people the virtual reality appears as something immaterial, and in some level autonomous. There are people who expect that some digital gadgets, mobile applications, or other computer systems will "know better" how to creatively respond to their needs and will autonomously take a proper action.[18]

From that perspective, cyber-weapons appear as uncontrollable and therefore have special moral status. In general, a tool itself cannot be morally responsible for the evil that is caused by its misuse. However, there are some tools more dangerous than others. The call to disarmament present since the Cold War was ended, confirms that nuclear weapons (similarly as the biological weapons) have a status ethically different from other conventional weapons. Cyber-weapons have some similarities to the biological weapon, i.e. they have the ability for uncontrolled and unintentional attack on properties far

[16] Kim Zetter, "Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report," *WIRED*, November 30, 2011, http://www.wired.com/2011/11/water-pump-hack-mystery-solved/

[17] Meme is a term introduced by Richard Dawkins in his work *The Selfish Gene*. Meme is a unit of cultural information spread normally by copying. See more about that term at Britannica Academic, "Meme," accessed December 16, 2015, http://academic.eb.com/EBchecked/topic/1655585/meme

[18] Cook, "Is There Anything Morally Special about Cyberwar?," 23–25.

away from the target aimed. For example, the Stuxnet worm affected Siemens centrifuges installed also outside of Iran.[19]

Under the term of neo-reality Cook understands some new way of perceiving reality by people living in both physical and virtual worlds. He presents an example of Google Glass, a prototype project of so called augmented reality. That technology brings elements from the digital world to our physical reality in the way that virtual elements permeate the real world almost imperceptibly. In other words, virtual reality becomes an important and indistinguishable element of our everyday life. In the case of cyberwar, that characteristic of the network creates the possibility of illegitimate manipulation of perception. It is predictable that the interpenetration of cyberspace into the physical world will progress. Hence, the threat of cyberwar becomes a fundamental danger for modern culture.

In Cook's opinion, the study of ethics in cyberwar may be enriched by the achievements of the debate about the ethics of nuclear weapons. Cyberwar shares at least two characteristics with atomic weapons: ubiquity and uncontrollability. Both cyberwar and nuclear war, in anyone's imagination can create an irrational threat. Both, cyberwar and nuclear war are not very precise in aiming at the target and easily affect the lives of innocent citizens. Naturally, it is only an analogy, because cyberwar had not developed into such lethal weaponry as the atomic bombs dropped on Hiroshima and Nagasaki in 1945.[20]

That analogy permits us to consider cyberwar as a tool of threat rather than weapon of direct attack. In the JWT there is a place for the use of threat as one of the last resorts to preserve peace. However, classical JWT does not discuss the effects of fear in a society. That topic was studied during the Cold War. One of the most significant documents that developed the ethics of fear is the Pastoral Letter of the U.S. Catholic Bishops published in 1983. In that document the bishops discuss an ethical approach to the use of fear as a tool of war. They talk about the culture of fear as a state of civilization that makes normal life impossible, even if the fear prevents a direct aggression. Therefore, the use of fear, even in a case of preventing direct aggression seems to be ethically questionable.[21] I develop more

[19] Cook, "Is There Anything Morally Special about Cyberwar?," 26.

[20] Cook, "Is There Anything Morally Special about Cyberwar?," 29-30.

[21] U.S. National Conference of Catholic Bishops, *The Challenge of Peace: God's Promise and Our Response*, Washington, DC: U.S. Catholic Conference Office of Pub. Services, 1983, para. 106.

deeply the statement of the U.S. Catholic Bishops in the following section.

With the end of the Cold War, politics found a way to build an international agreement on progressive nuclear disarmament. Would this be possible in the case of cyber warfare? The moral condemnation of indiscriminate threat might help to lead to this process. Even if our digital context is different from the context of the Cold War, the strategies and achievements of that time may be used in order to limit the escalation of cyber-violence. The role of international diplomacy seems to be an important factor in that process.[22]

Two approaches presented above, one of Larry May, and the second of James L. Cook, are very different in their argumentations. However, the proposed solution of both of them is convergent. Both of them argue that the most ethical solution to the problems of cyberwar can be solved by intensification of the diplomatic efforts. May proposes to change the language used in relation to cyberwar, and instead of a war to call it an embargo. That change, in his opinion, could better adjust the proportional response to a cyber-attack and would efficiently limit the escalation of cyber-violence. Cook shows the ethically singular status of cyberwar that makes them similar to nuclear warfare. He claims that diplomatic strategies from the recent Cold War, which led to the signing of the nuclear disarmament treaty, may be efficiently used in the case of cyberwar. Moreover, he notes the special contribution of the Letter of the U.S. Bishops to that process. This raises the question: can religious organizations contribute in efforts to develop some solution for cyber-peace? In the following section I study that topic.

3. The Ethics of Cyberwar from the Catholic Perspective

Religious institutions were often a place for ethical study and the source of moral principles for society. The churches frequently spoke out about various personal or social moral issues, and often were giving an interesting insight from a perspective hardly accessible for civil organizations. The Catholic Church, in particular, developed a rich study of the ethics of social issues, since 1891, when the Pope Leo XIII published *Rerum Novarum.* That long history of the development of thought, and different perspective based partially on spirituality rather than on pure rationality, makes

[22] Cook, “Is There Anything Morally Special about Cyberwar?,” 32.

Catholic Social Ethics an interesting source for study about the ethics of cyberwar.

The Catholic Church has not published any special document dedicated to the phenomenon of cyber warfare. However there are two documents that, in my opinion, can contribute to the development of ethics in that area. The first one is the document of the Pontifical Council for Social Communications, "Ethics in Internet" (2002). The second one was mentioned before: the Pastoral Letter of the U.S. Catholic Bishops *The Challenge of Peace: God's Promise and Our Response* (1983). Since neither of those documents refers directly to cyberwar, I present my own application of their content to that new phenomenon.

3.1. The Ethics in Internet

"Ethics in Internet" posits the human person and the human community as a fundamental principle, following the previous document "Ethics in Communications." "The human person and the human community are the end and measure of the use of the media of social communication; communication should be by persons to persons for the integral development of persons."[23]

Moreover, the document recalls two principles of Catholic Social Teaching, the principle of the Common Good, and the principle of Solidarity, as important moral factors for the network. Globalization and its effects, both, positive and negative are also visible in the internet. Especially alarming is growing inequality both in the economic sense and understood as a digital exclusion. Therefore, global solidarity in the service of the common good has to be applied in order to create an environment of human development in justice, peace and love.[24]

Those principles find a particular application in the ethics of cyber warfare. Cyberwar can limit human development and significantly augment digital exclusion. Cyber attacks are normally directed to damage or destroy the targeted systems. They create a direct loss of property, raise the cost of security, and cause threat and mistrust of

[23] Pontifical Council for Social Communications, "Ethics in Communications," June 2, 2000, para. 21, http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20000530_ethics-communications_en.html; quoted in Pontifical Council for Social Communications, "Ethics in Internet," February 22, 2002, para. 3, http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_en.html

[24] Pontifical Council for Social Communications, "Ethics in Internet," para. 5.

the new technologies. In the case of small or underdeveloped countries it may slow down or even stop their growth. The example of the cyber-attack in Estonia shows how dangerous it was for the sustainability of the country. The Center of Excellence on Cyber Defense established by NATO in Tallinn in 2008, in my opinion, is an example of the realization of solidarity and the care of common good. However, the responsibility of cyber-security should not be limited only to the allies of military pacts. I believe that the UN should strengthen its efforts to research and develop specific solutions in the field of network security.

One of the effects of globalization is a shift of power from countries to transnational corporations. Those companies, through development of modern technologies, have a fundamental influence on the shape and security of the network. They also play an important role in the domain of cyberwar. Most cyber-attacks are directed to the weak points, bugs, holes, and other malfunctions of the software or hardware. The economic race and the users' preference of new functions over the security causes lowering the quality standards of the offered computer systems, augment their vulnerability, and create a place for future cyber-attacks. That approach cannot be reconciled with the principle of the common good. The economic factor cannot be the only goal for those corporations. Responsibility for the later functionality of systems is in the hands of their developers. They should design some quality standards and other regulations to ensure the cyber-security of users. State or international intervention in some cases may be required.

Furthermore, the "Ethics of Internet" treats the idea of freedom on the network. The decentralized organization, ease of connection, and communication free of charge on the internet creates a feeling of unlimited liberty. That freedom, on one hand, gives an enormous boost to the development of cyber-civilization but, on the other hand, reinforces the influence of radical libertarianism, which holds that whatever is possible is permitted. In other words, radical libertarianism is against any limitations, even if that may lead to serious moral misconduct such as children's pornography, hatred, violence and cyber-violence. The document underlines that freedom is a mean to search for the truth and cannot be a goal in itself. Hence, the position of radical libertarianism cannot be reconciled with the principle of solidarity and of common good.[25]

[25] Pontifical Council for Social Communications, "Ethics in Internet," para. 12-14.

The application of this approach to the domain of cyberwar can bring another insight for the ethics of individual hackers, and of organized cyber-security experts.[26] The knowledge that they usually possess, and limitless possibilities to use it on the network give them a very privileged status. Frequently, it is their decision that makes the quality of connection better or worse. Their action can solve some problems or create new ones. Therefore their decisions should always be subjected to ethical judgment, and take in to account solidarity and care for the common good.

The last part of the document presents recommendations for the ethical development of the internet. It shows the importance of education, the necessity of internet regulations, and international cooperation. Finally it addresses some questions such as privacy, surveillance, cyber-terrorism, copyright, women rights, and digital division, that are still open and in need of international consensus.

3.2. The Challenge of Peace

The letter of the U.S. Catholic Bishops, titled *The Challenge of Peace: God's Promise and Our Response,* presents a deep study of Catholic Social Teaching regarding war and peace in the context of nuclear weapons. Although the topic of the document does not refer to the cyberwar, the unique ethical status of that new reality makes it possible to use an analogy to the nuclear warfare, as was previously presented in the paper of James L. Cook.[27]

In the beginning of the letter the bishops present the Christian theology of peace. Both approaches, biblical and theological, show peace as a realization of God's will, progress towards the Kingdom of God, and a moral obligation of Christians.[28] The document, citing the Pastoral Constitution *Gaudium et Spes*, says that peace is an indispensable condition for the construction of a world more genuinely human.[29] Moreover, peace is a condition for freedom in

[26] "Hacker," in my opinion, does not necessary mean a criminal. There are independent communities of computer experts, who call themselves "hackers," whose principal interest is to creatively develop new digital ways of thinking and not to harm anybody. There exist even some informal hacker's codes of ethics. Those hackers can be very efficient in the discovery and repair of system vulnerabilities and in preventing cyber-attacks. More about the Christian vision of hackers can be found in Antonio Spadaro, *Cybertheology: Thinking Christianity in the Era of the Internet*, New York: Fordham University Press, 2014, 51–70.

[27] Cook, "Is There Anything Morally Special about Cyberwar?," 31.

[28] U.S. National Conference of Catholic Bishops, *The Challenge of Peace*, para. 55–64.

[29] Vatican Council II, *Gaudium et Spes, Pastoral Constitution on the Church in the Modern World*, 1965, para. 77, http://www.vatican.va/archive/hist_councils/

any moral choices. The Christian understanding of peace does not limit itself only to the absence of war, but is progress toward harmony and justice. In other words, peace is not a state but a process that involve everyday effort.[30]

In the following section the letter analyses the traditional Christian approach to the Just War Theory. The document mentions the principle of self-defence and the Just War criteria: *Jus ad Bellum* (just cause, competent authority, comparative justice, right intention, last resort, and probability of success), and *Jus in Bello* (proportionality and discrimination).[31] Especially the last two principles, proportionality and discrimination, find special significance for the reality of cyber warfare.

The criterion of proportionality refers to the moral obligation to use defensive or preventative weapons that do not overcome the methods of the attacker. In other words, the response to an attack cannot do more harm than the attack itself. In the case of cyberwar it would mean that the response on the cyber attack that uses military force would be immoral. Still, the question remains, how could underdeveloped countries respond to a cyber attack? A possible realization of the principle of proportionality in cyber armament would be an international agreement about equal distribution of security systems, together with the necessary training.

The criterion of discrimination says that innocent civilians should not be harmed during a military operation. The ubiquity and uncontrollability of cyber-attacks, discussed by Cook, makes it difficult to fulfil that principle. In the attack on Estonia in 2007, the intended target was almost exclusively civil institutions. Even the well-designed Stuxnet worm depended on computers that belonged to private persons, and indeed affected systems far away from Iran. The problematic also includes a possible defence. In a hypothetical situation, the most efficient way to respond to a remote attack would be to disconnect the whole city or country from the internet. However, that solution would heavily affect civilians, hence the criterion of discrimination would be abused. It is controversial whether any active defensive cyber-weapon would be moral in that case.

ii_vatican_council/documents/vat-ii_const_19651207_gaudium-et-spes_en.html; cited in U.S. National Conference of Catholic Bishops, *The Challenge of Peace*, para. 65.

[30] U.S. National Conference of Catholic Bishops, *The Challenge of Peace*, para. 68.

[31] U.S. National Conference of Catholic Bishops, *The Challenge of Peace*, para. 68.

Moreover, the bishops underline the value of non-violent solutions and the role of the whole society in the construction of peace.[32] There are many ways in which society movements may in non-violent ways participate in cyber-conflicts. The internet itself helps to organize and accelerate social movements. The viral actions that reveal unjust practices, boycotts, or even public protests, in some situations may be an effective strategy against cyber threats. But the internet is a good place to promote safe and peaceful solutions as well. For example, the Open Source initiative for decades provides a high quality and safe software, thanks only to the dedication of independent enthusiasts. The new crowd-founding hubs such as kickstarter.com may effectively boost the creativity and accessibility of the safe and efficient solutions.

In my opinion, the main achievement of the letter of the U.S. Bishops is the shift in a perspective of looking at the nuclear threat. Their message is focused on promotion of peace instead of only the dark reality of war. The main goal, in their opinion, is not to only avoid a war but to develop a progressive peace based on global justice. I believe that this approach should be applied to the reality of cyber warfare. In other words, instead of looking for a justification of military cyber-operations, we should search for ways to create justice and peace in cyberspace. That goal cannot be realized apart from the real world. Poverty, social, economic and digital exclusion, race or national inequalities, and all others sources of injustice will find their expression in the cyberspace. Therefore, the solutions already developed at some level may and should be applied to cyberspace.

4. Conclusion

As I tried to show in the first section cyber warfare is present in our reality. The formal definition and classification of a particular cyber-activity as a war in cyberspace causes many difficulties. However, there are examples of events that earned the title of cyberwar. The involvement of international agencies and national diplomacies proves that cyberwar is an actual issue that requires an ethical evaluation.

There are various approaches to that evaluation. Both examples that I have offered in the second section lead to diplomatic solutions as the most ethical. In the opinion of Larry May, the change of language used for describing international cyber-violence may

[32] U.S. National Conference of Catholic Bishops, *The Challenge of Peace*, para. 117.

facilitate that solution. James Cook argues that solutions developed for nuclear threats during the Cold War may be useful also for cyber-threats. He cites the U.S. Catholic Bishops' letter as an important example of complete ethical vision on nuclear war and proposes its partial application to cyberwar.

The Catholic Church has not developed any document dedicated directly to cyber warfare; however, her achievements in social ethics can provide some new light for the ethical study of that problem. The Church's vision is based on hope that peace is possible. She puts the human person and the human community at the centre of her ethics. The two traditional principles of solidarity and of the common good find effective application in the ethics of cyberwar. Application of those principles led me to develop some particular proposals that I present in the third section. Moreover, the change of focus presented in the letter of US Catholic Bishops allows us to treat cyberspace as an instrument of peace rather than a tool of war.

The internet was designed in the late 1970s as a military project. It should not surprise us that it became a tool that is used to fight. Nonetheless, it is not the tool itself but its users that take ethical decisions and make it an instrument of war or peace. The internet, in contrary to a nuclear weapon, has a very rich variety of positive and peaceful applications. It connects people, provides a freedom never before accessible, reinforces social ties, is a place of education, work and entertainment, allows us to meet others and even to fall in love, and has so many other positive ways of use. In other words, the internet is a common good and helps us develop a global solidarity. Let us intensify our efforts to progress toward more peaceful and more just cyberspace.