GPSG Working Paper #07

Cyber-Security and the Law of War:
The Legal and Ethical Aspects of Cyber-Conflict

Dr. Andrew Liaropoulos
Lecturer in International Relations and Strategy
Department of International and European Studies
University of Piraeus

Abstract

Over the last years there is a growing body of literature over exploiting cyberspace for offensive and defensive purposes. Cyber-conflict is after all the newest mode of warfare and cyber-weapons have been described as weapons of mass disruption. Although the attention on the technical and military dimensions of cyberspace is justifiable, one needs also to look into the legal and ethical aspects of cyber-conflict, in order to comprehend the complex nature of cyberspace. The lack of an international legal framework that defines the use of force in cyberspace, operational difficulties in deterring and identifying cyber-attacks as well as the asymmetric dimension of cyber-conflicts pose without a doubt, great pressure on both theorists and practitioners of warfare. This paper will highlight the legal and ethical dilemmas regarding the use of force in cyberspace and question how the Law of War can be applied to cyber-threats.

Keywords: *war, law of war, ethics, just war theory, cyber-conflict*

Author Bio: ***Dr Andrew Liaropoulos*** *is a Lecturer in the Department of International and European Studies at the University of Piraeus, Greece. He also teaches in the Joint Staff War College, the National Security College, the Air War College and the Naval Staff Command College. His research interests include international security, intelligence reform, strategy, military transformation, foreign policy analysis and Greek security policy.*

1. Introduction

The Information Revolution has transformed not only the way society functions, but also the way war is conducted and a new type of conflict that takes place in cyberspace has emerged (Toffler 1993). Cyber-conflict is one of the greatest threats to international security and has become a part of modern warfare. Cyber-attacks are rapid; they cross borders and can serve both strategic and tactical goals (Liaropoulos 2009). Militaries and terrorist groups now have the capability to launch cyber-attacks not only against military networks, but also against critical infrastructures that depend on computer networks. Critical infrastructures consist of the physical and cyber assets of public and private institutions in sectors like water, public health, emergency services, executive government, defense industrial bases, information and telecommunications, energy, transportation, banking and finance. Cyberspace is the nervous system of all these infrastructures.

Recent cases of cyber-attacks in Estonia in April-May 2007 and Georgia in August 2008 confirm that the conflict spectrum has expanded and includes cyberspace as well (Blank 2008). The Estonia cyber-attack, which primarily targeted commercial financial networks, shut down the heavily online Estonian banking system for several days. The cyber-attacks in Georgia defaced the presidential website and made other government websites unavailable. Georgia was unable to communicate on the Internet for days and relocated cyber-assets to the United States, Estonia and Poland (Korns and Kastenberg 2009). Cyber-conflict is primarily disruptive, rather than destructive; and its low entry cost makes it possible for states, terrorist groups (Bunker 2000) and even individuals to acquire cyber-conflict capabilities with relative ease. Cyberspace is accessible to all and therefore makes conflict more thinkable. The less lethal appearance of cyber-conflict and the possibility of concealing the attacker's true identity (plausible deniability) put serious pressure on every war-related aspect.

The paper will first define the terms cyberspace and cyber-conflict, in order to describe the context under which cyber-attacks take place. After that, the existing Law of War will be applied to cyber-threats. In particular, the concept of just war theory will be used in order to explore the challenges that states face in responding to cyber-attacks.

2. Cyber-Conflict and the Law of War

Cyberspace refers to the fusion of all communication networks, databases and information sources into a global virtual system and cyber-conflict is defined as cyberspace-based attacks on the civilian and military infrastructures (transportation, power, communications and financial infrastructures) upon which societies and armed forces increasingly depend. Cyber-conflict is defined as "the conduct of large scale, politically motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks and infrastructures" (Mulvenon 2005). Cyber-related terms are hard to define and due to the nature of cyberspace (anonymity and plausible deniability), it is very often difficult to discern between cyber-conflict, cyber-war (cyber-based confrontation between states), cyber-espionage and cyber-terrorism.

By definition, cyberspace is transnational, thus cyber-conflict raises several issues related to sovereignty and security in the international realm. Furthermore, due to the potentially strategic impact of an attack, cyber-conflict must be treated as a subset of the larger literature about war and security (Mulvenon 2005). As a new realm that encompasses fast-moving new technologies for both states and non-state actors, legal and ethical aspects of cyber-conflict need to be further explored. The most important set of issues relate to the legal definitions of cyber-conflict and the implications of conflict in cyberspace for civilian, military and economic networks. In particular, when does a cyber-conflict constitute a use of armed force[1] or an actual act of war? Can a cyber-attack constitute an armed attack? What actions would constitute a war crime in cyberspace? What is appropriate self-defence in cyberspace? Is it possible to successfully attribute another state's responsibility for a cyber-attack? How can a state prevent cyber attacks originating from its territory (Graham 2010)?

Throughout history, the just war tradition has provided us with one of the most perpetual frameworks for the question of when it is right to go to war and how war ought to be conducted. In general, just war theory attempts to conceive of how the use of arms might

[1] Note that "use of force" is deemed an armed attack when the force is of sufficient scope, duration and intensity.

be restrained, made more humane, and ultimately directed towards the aim of establishing lasting peace and justice. Just war theory is probably the most influential perspective on the ethics of war and peace and drives its inspiration from the writings of Augustine, Aquinas, Grotius, Suarez, Vattel, Grotius and Waltzer. The reason that we need a just war theory is that we live in a non-ideal world, where war might be ethically inescapable. Therefore, the purpose is to give some wars legal and moral justification, to condemn those that do not comply with the criteria and impose restrictions on the actual conduct of war. Just war theorists have traditionally concerned themselves with the grounds for going to war in the first place and with questions about ethical conduct in warfare (Waltzer 2000, Evans 2005).

Therefore, the just war theory can be divided into two areas. The first one, jus ad bellum, refers to the transition from peace to war and basically lays out when states may lawfully resort to armed conflict. The second one, jus in bello, also known as the law of armed conflict, refers to the actual use of force during war. Therefore, the key concepts of just war theory fall into the categories of criteria for going to war (jus ad bellum) and of fighting justly during war (jus in bello).

The jus ad bellum criteria are: *Right Purpose.* Reasons for going to war revolve around the concept of self-defence, which Article 51 of the United Nations Charter deems an “inherent right”. Notions of right purpose generally also include ideas like pre-emption, but are less open to the idea of preventive war. *Duly constituted authority.* A necessary condition for having a just war is that the decision to fight must come from a government, or a coalition of states, not from an individual. *Last resort.* War cannot be considered just unless it follows exhaustive pursuit of negotiations and other means of conflict resolution (Arquilla 1999).

The jus in bello criteria are: *Noncombatant immunity.* According to just war theory, those waging the war must strive to avoid harming civilians or enemy troops that have surrendered. *Proportionality.* When waging war, force must be applied in a manner that avoids excessive use. A state in self-defence will use the amount of force that is required to defeat an ongoing attach or deter a future one. *More good than harm.* When force is used, the ethical conduct requires calculation of the net good to be achieved by a particular use of force (Arquilla 1999).

The absence of international rules that define the use of force in cyberspace (Delibasis 2002), and technical difficulties in identifying cyber-attacks challenge every aspect of just war theory. Uncertainty and confusion have always been part of the battlefield and the same applies for the cyberspace. The implications of uncertainty are most pronounced for deterrence. Deterrence depends on the threat of retaliation to change the opponent’s calculus of the benefits and costs of an attack. But it is hard to convincingly threaten an unknown cyber-attacker. Likewise, uncertainty about collateral damage will affect decisions by political leaders, who may be unwilling to incur the risk of a cyber attack that could widen or escalate a conflict (Lewis 2009). This uncertainty also affects the ethics of conducting cyber-attacks. Over the past years, the just war-fighting issues have gained the attention of political scientists (Schmitt 2002, Pretorius 2003, Rowe 2008). Recent doctrinal developments and governmental initiatives for the protection of critical infrastructure necessitate a thorough analysis of the way just war theory can be applied in cyber-conflict. Following the 2007 cyber-attack on Estonia, NATO began to invest in the defense of cyberspace, and Allied nations have acknowledged the need to secure networks.

The range of operations that might make use of cyberspace extends broadly, from the battlefield to the enemy home front. Cyber-conflict scenarios include attacks on both the software (logic bombs, computer viruses, etc) and hardware (electromagnetic weapons). Cyber-conflict may serve as a form of close support for military forces during active

operations. It may also be employed in strategic campaigns designed to strike directly at the will and logistical support of an opponent.

In addition, it is important to note the inherent blurriness with regard to defining combatants and acts of war. Whereas in other types of warfare, it is quite clear who is making the attacks, in cyber-conflict, almost anyone can fight. Thus, it is important, from an ethical perspective, to make a distinction between those with access to advanced information technology and those using it for purposes of waging cyber-attacks. Further, the very nature of cyber-attacks is such that it may often be difficult to discern between criminal, terrorist, and military acts.

The danger of cyber-attacks is greatest for those most dependent on electronics. In both cases, whether applied in the battlespace or the civilian infrastructure, the more electronically-dependent an actor is, the more vulnerable it is. Both technologically advanced armies and technologically advanced countries are more vulnerable than those that are less developed. Furthermore, in a future conflict against guerrilla fighters that use conventional weapons, directed-energy bombs are useless. But they are obviously not useless against an army that is dependent on information technology.

Under existing just war theory, prevention lies on shaky ground. But cyber-conflict might prove especially useful in derailing the rise of a threatening power - particularly those forms of attack that might be necessary in slowing down a potential adversary's process of proliferation of weapons of mass destruction. Regarding duly constituted authority, the very nature of weaponry may challenge this long-established ethical concept. For the types of capabilities needed to conduct a cyber-campaign (especially in the cases of attacking software) there is little need for traditional forces.

Although there are plans for the creation of cyber-corps, almost anyone can become a cyber-warrior. Therefore, the state monopoly on war reflected in the concept of duly constituted authority will likely be shaken, as non-state actors rise in their ability to wage cyber-war (Arquilla 1999). The ease of entry into the realm of cyber-conflict also suggests that the convention regarding going to war only as a last resort will come under strain. Cyber-attacks may disrupt much, but they do little actual destruction and therefore can be viewed as somewhat akin to economic sanctions, as a tool of coercion.

Cyber-attacks that strike an adversary's infrastructure must be seen as a kind of war that targets non-combatants in a deliberate manner. They will suffer, inevitably and seriously, from such attacks. In common with strategic aerial bombardment, the purpose is to undermine the enemy's will to resist. Another problematic issue is proportionality. In particular, a cyber-attacker might strike at an opponent's critical infrastructures, but have few or none of his own that could be retaliated against by similar means. This prompts the question of when more traditional military measures - including some degree of lethal force - might be used in response to cyber-attacks without violating notions of proportionality.

Alike, another problem arises if the defender/target that is struck by cyber-weapons has little or no means of responding with the same cyber-weapons (Arquilla 1999). Massive retaliatory threat may be the only credible deterrent that a potential victim of cyber-conflict may have. Therefore and despite its less lethal profile, cyber-conflict might trigger a potentially bloody conflict. Despite the widely held belief that the nature of cyber-attacks is disruptive and not destructive, and therefore cyber-conflict is less life-threatening than a kinetic weapon, the dissemination of cyber-capabilities, can actually have the opposite effect. In particular, the fact that cyber-attacks may be cheaper and easier to conduct in the

near future, might actually increase the number of conflicts, both in and outside cyberspace. This will inevitably increase the number of casualties.

Aside from deliberately disproportionate responses, there is also the problem of estimating the comparability of damage done by radically differing weapons systems (exploding smart bombs *vs* computer logic bombs). Finally, the problem of perpetrator ambiguity further weakens proportionate response, as one may simply not have enough data to determine just who is responsible for a particular attack.

3. Defining and responding to cyber-attacks

Cyber attacks come in many different forms, and their destructive potential is limited only by the creativity and skill of the attackers behind them. The cyber-conflict battlefield is comprised of many components that include the Internet and all things that connect from a computer to the Internet. This would include: web servers, enterprise information systems, client server systems, communication links, network equipment, and the computers in businesses and homes. The terrain also encompasses information systems like the electrical grids, telecommunication systems, and various corporate and military robotics systems.

As a result there is a broad typology of cyber-attacks. Some of the most common are cyber-espionage, web vandalism, denial of service (DOS) and attacks on critical infrastructure. Cyber-espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers. Web vandalism involves attacks that deface web pages, or denial-of-service attacks, where a large number of computers are controller by one actor. Finally, attacks on computer networks that involve power plants, water supply stations, communications hubs, and commercial infrastructure facilities are high on the security agenda.

Although certain cyber attacks can constitute armed attacks, especially in light of their ability to injure or kill, the legal community has been reluctant to adopt this approach because cyber attacks do not resemble traditional armed attacks with conventional weapons. Technically cyber-attacks are difficult to attribute and as a result scholars and practitioners have developed analytical models to evaluate such unconventional attacks and equate cyber-attacks with armed attacks (Carr 2010, Graham 2010).[2] For example, a cyber-attack that shuts down a power grid is an armed attack. The reason is that shutting down a power grid requires dropping a bomb, or the use of some other form of kinetic force. Since cyber-attacks are used to achieve the same result with conventional attacks, they are therefore treated the same way as armed attacks. A cyber-attack that temporarily interrupts service of another state's local phone company and causes some hundred people to be without a phone, does not amount to an armed attack. On the contrary, a cyber-attack that compromises the control system of a chemical or biological plant, and thereby causes the release of toxic gases over a city, is equivalent to an armed attack (Joyner and Lotrionte 2001). Likewise, a cyber-attack that manipulated information across a

[2] There are three analytical models that determine whether a cyber-attack constitutes an armed attack. The 'instrument based approach' that examines whether the damage caused by a cyber-attack could previously have been achieved only by a kinetic attack, the 'effects based approach' that examined the overall effect of the cyber-attack on the victim state and finally the 'strict liability' approach that deems every cyber-attack against a nation's critical infrastructure as an armed attack. For more details see the works of Carr and Graham.

state's banking and financial institutions to seriously disrupt commerce in the state is an armed attack. The logic is that the disruptive effects that the attack had on the state's economy is a severe enough overall consequence that it warrants treatment as an armed attack (Carr 2010).

A scholar that advocated such analytical models is Michael Schmitt. His analytical framework for evaluating cyber-attacks, discerns six criteria: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy (Schmitt 1999). *Severity* looks at the scope and extent of an attack. So, if people are killed or there is extensive property damage, the action is considered an armed attack, the less damage, the less likely the action is a use of force. *Immediacy* examines the duration of the effects of a cyber-attack. The longer the duration and effects of an attack, the stronger the argument that it is an armed attack. *Directness* refers to the harm that is caused. If the action taken is the sole cause of the result, it is more likely to be viewed as a use of force. *Invasiveness* looks at the origin of the attack. A violated border is still an indicator of military operations; actions that are mounted from outside a target nation's borders are probably more diplomatic or economic. *Measurability* quantifies the damage. If the effect can be quantified immediately, it is more likely that it will be considered as an armed attack. Finally, *presumptive legitimacy* focuses on state practice. The less a cyber-attack looks like accepted state practice, the more possible it is that it will be regarded as an armed attack (Schmitt 1999).

Despite the fact that Schmitt's six criteria have gained wide acceptance in the legal community, technological limitations on attack detection and attack classification, make states hesitant to adopt these criteria with relative ease and characterize all cyber-attacks as armed attacks (Carr 2010). Jus ad bellum requires states to ensure that the cyber-attack originates from a sanctuary state. Only then can a state lawfully respond. The problem is that cyber-attacks are frequently conducted through intermediate computer systems to disguise the true identity of the cyber-attacker. As a result, trace programs run the risk of incorrectly identifying the true source of an attack. This creates an apparent problem because an attack could be incorrectly perceived as coming from a state that is not the actual state of origin (Carr 2010).

4. Conclusion

Information societies are build around critical information infrastructures, that are easy to access, friendly to use, but also vulnerable to cyber-attacks. Modern armies develop advanced capabilities in cyberspace. These capabilities are focused not only on collecting sensitive information, but also on achieving military effects capable of causing economic harm, damaging critical infrastructure, and influencing the outcome of conventional armed conflicts. Thus, a major challenge for national governments and global organizations is to secure cyberspace, while maintaining an open society, all carried out through lawful and just means.

The use of just war theory as a theoretical framework, for the analysis of cyber-conflict, revealed that international law must define more sharply the criteria that characterize cyber-attacks as equivalent to armed attacks. The recent cyber-attacks in Estonia and Georgia, stress the need to define what sort of responses are permissible as self-defense by a state that is targeted. The Law of War must evolve and adapt, because cyber-warriors, have taken the threat out of the realm of the abstract and made it real.

Bibliography

Arquilla, J. (1999) "Can Information Warfare Ever be Just?", *Ethics and Information Technology,* Vol 1, pp 203-212.

Blank, S. (2008) "Web War I: Is Europe's First Information War a New Kind of War?", *Comparative Strategy,* Vol 27, No.3, pp 227-247.

Bunker, R. (2000) "Weapons of Mass Disruption and Terrorism", *Terrorism and Political Violence,* Vol 12, No.1 pp 37-46.

Carr, J. (2010) *Inside Cyber Warfare,* O'Reilly, Beijing.

Delibasis, D. (2002) "The Right of States to Use Force in Cyberspace: Defining the Rules of Engagement", *Information & Communication Technology Law,* Vol 11, No.3, pp 255-268.

Evans, M. ed. (2005), *Just War Theory. A Reappraisal*, Edinburgh University Press, Edinburgh.

Graham, D. (2010) "Cyber Threats and the Law of War", *Journal of National Security Law Policy*, Vol 4, pp 85-100.

Joyner C. and Lotrionte C. (2001) "Information Warfare as International Coercion: Elements of Legal Framework", *European Journal of International Law,* Vol 12 No.5, pp 825-865.

Korns, S. and Kastenberg J. (2009) "Georgia's Cyber Left Hook", Parameters, Vol 38, pp 60-76.

Lewis, J. (2009) "The Fog of Cyberwar. Discouraging Deterrence", International Relations and Security Network (ISN), last accessed 20 January 2010, http://www.isn.ethz.ch/isn/layout/set/print/content/view/full/22009.

Liaropoulos, A. (2009) *The Transformation of Warfare in the Information Age*, Themata: Policy and Defence, No.28, Defence Analyses Institute, Athens.

Mulvenon, J. (2005) "Toward a Cyberconflict Studies Research Agenda", *IEEE Security & Privacy,* Vol 3 No.4 pp 52-55.

Pretorius, J. (2003) "Ethics and International Security in the Information Age", *Defense & Security Analysis*, Vol 19, No.2 pp 165-175.

Rowe, N. (2008) "Ethics of Cyber War Attacks", In: Janczewski, L.J. and Colarik, A. M. eds., *Cyber Warfare and Cyber Terrorism,* Information Science Reference, Hershey, pp 105-111.

Schmitt, M. (1999) "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Vol 37 No.885, pp 885-937.

Schmitt, M. (2002) "Wired Warfare: Computer Network Attacks and Jus in Bello", *International Review of the Red Cross,* Vol 84 No.846, pp 365-399.

Toffler, A. and H. (1993) *War and Anti-war: Survival at the Dawn of the 21st Century*, Warner Books, New York.

Waltzer, M. (2000) *Just and Unjust Wars: A Moral Argument with Historical Illustrations,* Basic Books, New York.

Williams, R. Jr. and Caldwell D. (2006) "Jus Post Bellum: Just War Theory and the Principles of Just Peace", *International Studies Perspectives*, Vol 7 No.4, pp 309-320.

Email: andrewliaropoulos@gmail.com