The effectiveness of the principle of distinction in the context of cyber warfare

by

LEANNE CHRISTINE VAN BREDA

A dissertation submitted in partial fulfilment for the Degree of

LL M in International law (RD) (M4042Q)

Faculty of Law

UNIVERSITY OF JOHANNESBURG

Supervisor: Prof. Mia Swart

2014

Contents

Introduction

International humanitarian law provides foundational norms which are to be observed by states in order to protect civilians from the harsh realities of war. These norms have been applied to traditional kinetic methods of warfare but as technology advances at a rapid pace so too do methods of warfare. As weaponry becomes more sophisticated it is necessary to revisit the foundational principles of international humanitarian law and apply them to situations that could only previously have been imagined. The principle of distinction is a core principle of this branch of law and it is not to be disregarded as a result of the fact that it predates modern methods of warfare but rather it is to be re-examined, its importance observed and applied to the warfare that we are faced with today. Protecting civilians has been of utmost importance in recent history and the development in the technology of weapons should not change that fact in the present or in the future.

Today it is possible to conduct war through computers located nowhere near the area in which is impacted by such attacks. This was unimaginable at the dawn of international humanitarian law but is a very real present reality. Cyber wars have already occurred in recent history and are often an attractive method of warfare for states as they have many beneficial advantages such as cheaper, less dangerous and more precise attacks without the disadvantages of losing soldiers and the expense of weapons.

As a result of the practical reality of cyber attacks in modern warfare, it is of great importance that the fundamental principle of distinction in international humanitarian law is analysed. To determine whether it is relevant in present day conflicts, the practical difficulties of applying the principle will need to be examined. The principle will only be effective where it protects civilians and as such it is necessary that it be established that civilians do indeed benefit from the principle. These issues will be addressed in Chapter One.

In order to fully comprehend the application of international humanitarian law to cyber methods of warfare, it is essential that fundamental knowledge of cyber war be understood. Definitions offer assistance in this regard and will need to be explained before further examination of this technical topic can proceed. As suggested above,

there are various reasons why state may prefer cyber attacks over conventional kinetic attacks such as bombing. The reasons for this will be explained in Chapter Two. Various instances of cyber warfare that have occurred in our recent history will also be examined.

After addressing the international humanitarian law principle of distinction and cyber warfare as a whole, it is necessary to apply the law to the scenario of cyber warfare which poses a situation slightly different to traditional application of the law to warfare. Through analysis of the International Strategy for Cyberspace, the Tallinn Manual and the *Nuclear Weapons* Advisory Opinion we find that the principle must be applied but this does not occur without problems. To a large extent these problems are similar to the problems faced with application to traditional wafare. What is of fundamental importance, however, is that civilians are afforded the maximum amount of protection possible and the fact that methods of warfare differ from previous methods in history should not affect this protection.

Chapter 1: Traditional principles of international humanitarian law

We live in a time where there has been more development in international law than any other time in history however civilians have in recent years become key targets of modern warfare. This juxtaposition is evidence of a gap existing between the normative rules of international law and practical realities of the battlefield. These realities are eroding the normative rules. The principle of distinction is an important principle protecting civilians. To understand the application of the principle of distinction in light of any warfare (including cyber warfare) it is necessary to consider a thorough examination of what is meant by this principle, its origin and the practical issues that may occur when applying the principle to various situations.

The Principle of Distinction

This principle lies at the core of the law of war and *jus in bello* and, as codified in Additional Protocol I of the Geneva Conventions, it is widely regarded as customary

international law.[1] The main objective of the principle is to protect those who are not participating in the war from its harsh realities. It prohibits *direct* and *intentional* attacks on civilians and non-combatants. Where civilians or non-combatants are affected as unintended collateral damage, however, suffering caused to them may be permissible only where the attack is necessary and proportional to military advantage. These supplementing principles qualify whether a target may be lawfully attacked.[2]

The principle of necessity is used to establish that there was a reasonable connection between the effects on those not party to the conflict and overcoming enemy forces.[3] The principle of proportionality prohibits attacks which might cause incidental loss of civilian life, injury to civilians or damage to civilian objects that would be excessive in relation to the military advantage that is anticipated.[4] The potential damage must be weighed against the benefit that could be gained from such an attack.[5] These age-old principles have formed the foundation of international humanitarian law.

The codification of the principle of distinction

The principle of distinction can be traced back to the preamble of St. Petersburg Declaration which states that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy."[6]

The Oxford Manual of 1880 states that war "does not admit of acts of violence, save between the armed forces of belligerent States."[7] The manual further states that this

[1] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) *opened for signature* 12 December 1977. Article 48.
Not all states are parties to the Geneva Conventions but due to its wide acceptance it may be accepted that it has received the *opinio juris* and state practice required to be afforded customary law status (especially Common Articles 2 and 3).
[2] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 734.
[3] Thürer *International Humanitarian Law: theory, practice, context* (2011) p68.
[4] Article 51.5(b) of Additional Protocol I.
[5] Aust *Handbook of International law* (second edition) 242.
[6] St. Petersburg Declaration 11 December 1868.
[7] The Laws of War on Land adopted by the Institute of International Law, Oxford, 9 September 1880. Article 1.

rule implies that there exists "a distinction between the individuals who compose the armed force of a state and its other 'ressortissants'".[8]

The Lieber Code, drafted during the American Civil War, was the first codification of the principle of distinction.[9] According to the Code unarmed citizens were to be spared "[*sic*] in person, property, and honor as much as the exigencies of war [would] admit."[10] This implied that the protection was not absolute. The realities of the Civil War, however, saw that civilians were in fact targeted creating a gap between the rules and practice which would continue throughout history.

Both the Lieber Code and the St. Petersburg Declaration have served as important models in the formation of Hague law.[11] The Hague Convention of 1907 prohibits attacks on undefended towns, villages and buildings further codifying the principle of distinction.[12] Undefended civilian objects are not to be attacked but undefended military objects are permissible objects of attack. These principles were not, however, adhered to in WWI or WWII. Rather, there was an increase on the attacks on civilians. Dresden and Tokyo were firebombed, London was targeted with rockets and Hiroshima and Nagasaki suffered nuclear weapon attacks, all with the intention of harming civilians.[13] The principle of distinction had been forgotten.

The International Committee of the Red Cross recognised this and intended to reintroduce the principle by expanding the Geneva Conventions with Additional Protocols I and II to include the principle of distinction which protects civilians from direct attacks by limiting legitimate targets to military objectives.[14] As mentioned above, these conventions have attained customary law status, thus entrenching the principle of distinction as a result of satisfying the requirements of settled practice

---

[8] The Laws of War on Land adopted by the Institute of International Law, Oxford, 9 September 1880. Commentary of Article 1.

[9] Instructions for the Government of Armies of the United States in the Field, General Orders No. 100 (Lieber Code) 24 April 1963.

[10] Article 22.

[11] Crowe, Weston-Scheuber *Principles of International Humanitarian Law* (2013) 31.

[12] Convention (IV) respecting the Laws and Customs of War on Land *signed at* The Hague 18 October 1907. Article 25.

[13] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 738-740.

[14] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) *opened for signature* 12 December 1977.
Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.

(*usus*) as well as *opinio juris*.[15] The fact that the distinction principle has reached customary international law status is of utmost importance in the realm of cyber war as will later be discussed.

Though these laws have attained customary status, they were again violated in the Gulf War and the Former Yugoslavia where "centres of gravity" were targeted. These comprised of bridges, highways, infrastructure, power plants, communication facilities, oil refineries and factories many of which offered dual purposes.[16] We can thus establish that history has revealed a gap between the norms and reality of the principle of distinction history which is problematic for application thereof and may continue to create problems in the realm of cyber war in future.

Present Day Practical issues

The principle of distinction is widely accepted as customary international law but despite its widespread acceptance, it is constantly violated by states and non-state actors. Recent conflicts have seen violations occur in the former Yugoslavia, Northern Ireland, Sudan and Rwanda.[17]

While the principle is met by unwillingness of States to abide by it, there also exist situations which make it difficult to obey. Many targets cannot be distinctly separated as either civilian or military objects but rather serve both those participating and those not participating in the conflict. Are objects that serve dual purposes permissible targets? Some civilians voluntarily contribute to armed conflict. Are these civilians afforded blanket protection purely because they are not part of the armed forces? Weaker parties to conflict might also be disadvantaged by the principle as it "entrenches the *status quo*, leading insurgents and weak states to

---

[15] "Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it." *North Sea Continental Shelf* 1969 ICJ Reports 3 at 44.
The International Court of Justice has held that some treaty rules, such as common Article 3 of the Geneva Conventions, have become customary international law. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* 27 June 1986 ICJ Reports 14 par 218.
Many provisions of Additional Protocol II to the Geneva Conventions may now be regarded as declaratory of rules of customary international law. Cassese, Acquaviva, Fan and Whiting *International Criminal Law cases and commentary* (2011) 13.

[16] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 *742.*

[17] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 735.

reject the law and wage war without constraints."[18] These are questions worth raising as they are grey areas not specifically provided for in treaty law and remain relevant to all types of armed conflict.

A. Dual purpose objects

The ICRC have provided in the commentary on the Geneva Conventions that only attacks made against objects directly used by armed forces (*example* weapons and equipment), locations of special importance for military operations (*example* bridges) and objects intended for use or being used for military purposes would constitute permissible targets.[19] This amounts to a strict interpretation of the principle.

The distinction between the civilian and military objects is, however, not always clear. Areas of ambiguity do exist. Power plants, bridges, transportation systems, factories and communication facilities are obvious examples of objects essential to both the military and civilians.

The United States, contrary to the ICRC, support a weak interpretation of distinction based on the enemy's centres of gravity and as such all dual-purpose objects may be targeted.[20] The problem, however, lies in the fact that the main aim of distinction is to protect civilians and by encompassing dual-purpose targets as legitimate military objectives, the aim of protection to be afforded to civilians is eroded. Weak interpretation could have serious consequences for civilians employed in production, logistics or communication assisting the military during conflict as it could mean that they become targets. To equate their employment with a military objective, however, is to stretch the principle of distinction to almost breaking point.[21]

Stricter interpretation allows only objects directly used by parties to the armed conflict or special military locations to be targeted.[22] If one observes this interpretation, dual-purpose targets are completely protected. This in itself poses the problem of providing *too much* protection as it could shield military objectives or even lead to intentionally mixing civilian and military objects to afford the military

[18] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 *742.*
[19] International Committee of the Red Cross, Commentary on the Additional Protocol of 8 June 1977 to the Geneva Conventions of 12 August 1949 636 (1987).
[20] United States Department of Air Force, USAF Intelligence Targeting Guide, February 1998 par 1.71.
[21] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 751.
[22] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 751.

advantage over other parties to the conflict.[23] It could also encourage the use of human shields.[24]

There is no settled interpretation of this issue and ambiguity surrounding dual-purpose objects erodes the principle of distinction.[25] The law needs to be sufficiently clear that it may be applied.

B. Civilians involved in direct hostilities

Civilians are protected so long as they do not take direct part in hostilities.[26] As stated above, however, civilians may be relied on by the military for certain services during armed conflict.[27] These civilians can be termed civilian contractors and all other civilians can be termed civilian settlers. Both are protected unless they engage in acts of war. Swiney suggests that civilian contractors are essential partners to the military.[28] The Geneva Conventions have recognised that certain civilians are more closely connected to conflict than others as certain civilians who have been involved in conflict are to be afforded prisoner of war status.[29] The principle of distinction, however, doesn't recognise this as all civilians are afforded protected status so long as they do not take part in direct hostilities.

Swiney suggests that civilian settlers of occupied lands are also fully protected by distinction even though their acts increased control over occupied land, so long as they have not taken part in direct hostilities.[30] He finds this to be illogical as while the

---

[23] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 751.
[24] Bosnian Serb forces used human shields to protect ammunition bunkers, radar sites and other military objects. Bassiouni *International Criminal Law: Sources, Subjects, and Contents* (3rd ed) 757.
[25] Final report to the prosecutor by the committee established to review the NATO bombing campaign against the Federal Republic of Yugoslavia, http://www.icty.org/x/file/About/OTP/otp_report_nato_bombing_en.pdf [last accessed: 17 December 2013 at 12:12].
The existing law was found to be too vague which resulted in the committee advising against prosecuting NATO forces.
[26] Article 51(3) Additional Protocol I to the Geneva Conventions.
[27] *For example* American forces, while occupying Iraq, employ Iraqi civilians as armed security guards, truck drivers, etc. Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 752.
[28] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 753.
[29] Article 4(4), 5 Geneva Convention (III) Relative to the Treatment of Prisoners of War, 12 August 1949. Supply contractors, war correspondents, civilian crews of military and civilian aircraft are to be afforded prisoner of war status.
[30] Such is the case with Israeli settlers in the West Bank and Jerusalem with the support of the government. A similar situation occurred in Sri Lanka whereby Sinhalese settlers were used to reduce Tamil control in Tamil dominated areas. Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 754.

tools of occupation are civilians, there is a military purpose which is shielded by the fact that civilians cannot be targeted.[31]

C. Ambiguity protects stronger parties

Economically stronger parties to the conflict are in a position to use advanced weaponry which protects their own combatants such as drones. They are able to use the ambiguity of dual-purpose objects to their advantage when this injures civilians. Where they apply a weak interpretation of dual purpose, targeting these objects is admissible. They can also contract civilians to assist in their purpose and use settlers as occupants and as such, a type of shield.[32] This leaves the weaker party in a position of asymmetrical conflict. Without advanced weapons, they have few legitimate military targets and this may lead them to abandon the principle of distinction so as not to be defeated. This may legitimise insurgencies in some cases.[33]

It is clear that there are obvious flaws in the application of the principle of distinction to modern warfare. It is of utmost importance, therefore, that we consider how exactly this principle is serving those it aims to; civilians.

How the principle of distinction affects civilians

International law today has evidenced a shift away from state sovereignty towards an emphasis on human rights of individuals. There is a separation which exists between *jus ad bellum* (the law regarding the resort to armed conflict) and *jus in bello* (the law governing the conduct during armed conflict).[34] While in the past more focus was given to *jus ad bellum*, victims of armed conflict still needed protecting which is why international humanitarian law applies equally and uniformly in situations of armed conflict today.[35]

---

[31] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 754.
[32] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 754.
[33] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 756.
[34] Von Sternberg "Yugoslavian war crimes and the search for a new humanitarian order: the case of Dusko Tadic" 1996 *St. John's J. Legal Comment* 351 353, 362.
[35] Cryer, Friman, Robinson, Wilmshurst *An introduction to international criminal law and procedure* (2007) 223-224.

Where civilians are directly targeted in violation of Article 51(2) of Additional Protocol I of the Geneva Conventions, this will constitute a grave breach and therefore the violation will be considered a war crime.[36] The Trial Chamber of the International Criminal Tribunal for the former Yugoslavia has held that attacks on civilians are also prohibited under common Article 3 of the Geneva Conventions which attained customary international law status.[37]

Jus cogens represents customary international law at its highest category and which may not be violated by States.[38] It has been suggested that any declaration on minimum humanitarian standards, including the principle of distinction, should be based on principles of *jus cogens*, expressing basic humanitarian considerations which are universally binding.[39]

Rules that previously applied only to international conflicts are today applicable to internal conflicts as a result of the status of *jus cogens* and the importance of human rights. Common Article 3 of the Geneva Conventions has been held by the International Court of Justice as codifying *jus cogens*.[40] The obligation to treat those not party to the conflict humanely, prohibition of certain inhumane acts as well as caring for the sick and wounded and, as such, the principle of distinction itself is now of fundamental importance.

Additional Protocol II of the Geneva Conventions ensures that the principle is also observed in non-international armed conflict as it provides the additional

---

[36] Article 85 Protocol Additional I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I) *signed on* 8 June 1977.

[37] *Prosecutor v Galic* Judgment Case No. IT-98-29-T ICTY Trial Chamber 5 December 2003.
The Trial Chamber has specifically qualified these attacks to be such that "are those launched deliberately against civilians or civilian objects in the course of an armed conflict and are not justified by military necessity...[and] must have caused deaths and/or serious bodily injuries within the civilian population or extensive damage to civilian objects." *Prosecutor v. Kordic and Cerkez* Judgment Case No. IT-95-14/2-T ICTY Trial Chamber 26 February 2001.
Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, The Prosecutor v Dusko Tadic Case No. IT-94-1-AR72 (International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed on the Territory of the Former Yugoslavia 1995). At par III, the Appeals Chamber extended customary international humanitarian law to internal conflicts as it held that fundamental human rights apply, the distinction between military operations and civilians is to be observed, no civilian dwelling is to be subject to attack, military attacks are not to take place in areas affording protection to civilians and civilians may not be forcibly removed.

[38] Article 53 Vienna Convention on the Law of Treaties 22 May 1969.

[39] Henckaerts, Doswald-Beck *Customary international humanitarian law, Volume II: Practice* (2005) 15.

[40] Miliatry and Paramilitary Activities In and Against Nicaragua (*Nicaragua v United States*) 1986 ICJ 4 105 par. 200.

requirements of protecting civilians against direct attacks, subjecting civilians to terror, destruction of property which they are dependent upon, damage to objects of cultural or religious importance and protection against forced removals.[41] This can be regarded as declaratory of existing rules of customary international law and *jus cogens*.[42]

The Vienna Convention maintains that *jus cogens* norms are recognised by the international community and bind all states.[43] No derogation of these norms is permissible. An act in contravention of these norms is void and states have an *erges omnes* obligation to bring violators to justice. Universal jurisdiction exists for any violation to these norms.[44] This further emphasises the utmost importance of the observance of this principle.

As further evidence of the protection afforded to civilians, the Genocide Convention was drafted after World War I to protect civilian groups from extermination.[45] The Convention criminalises the destruction of religious, national and ethnic groups by individuals and government officials where there exists a specific intention to do so.[46]

The former Yugoslavia presents one of many situations worth examining when considering the role of the principle of distinction in reality. Ethnic cleansing became a common military practice within Bosnia contrary to it being outlawed by international law. As a result civilians were deliberate targets of attacks in this region. The Bosnian government sought assistance from the United Nations in the form of collective security to prevent genocide but it was met by the international community's practice of non-intervention and passive measures of attaining peace.[47] Sanctions were enforced by the international community in the form of an Arms

[41] Article 13 – 17 Additional Protocol II of the Geneva Conventions.
[42] Cassese, Acquaviva, Fan and Whiting *International Criminal Law cases and commentary* (2011) 13.
[43] Vienna Convention on the Law of Treaties, 23 May 1968 (in force 27 January 1980). Article 64.
[44] Von Sternberg "Yugoslavian war crimes and the search for a new humanitarian order: the case of Dusko Tadic" 1996 *St. John's J. Legal Comment* 351 377.
[45] The Convention on the Prevention and Punishment of the Crime of Genocide 9 December 1948.
[46] Procida "Ethnic cleansing in Bosnia-Herzegovina, a case study: employing United Nation mechanisms to enforce the convention on the prevention and punishment of the crime of genocide" 1995 *Suffolk Transnat'l L. Rev.* 655 668.
[47] Procida "Ethnic cleansing in Bosnia-Herzegovina, a case study: employing United Nation mechanisms to enforce the convention on the prevention and punishment of the crime of genocide" 1995 *Suffolk Transnat'l L. Rev.* 655 674.

Embargo.[48] This aimed to curb the escalation of violence however it left Bosniaks unable to defend themselves against the already armed Serbs and Croats.[49] The Security Council stationed peacekeeping forces within Bosnia to provide protection against genocide.[50] Their presence in Sarajevo, however, was unable to contain the practice of ethnic cleansing. "Safe zones" for civilians were anything but as Serbs used these areas as targets for their aggression and there were insufficient peacekeepers to offer protection.[51] The Security Council also took measures to investigate and prosecute war crimes rather than assist with collective security, which did not immediately protect civilians.[52] It was only after the height of violence that the Security Council declared the genocide in Bosnia a threat to international peace and security and all necessary measures to insure peace could be taken.[53] This meant that political means to attain peace had been unsuccessful and that collective security could finally be implemented.

The principle has been blatantly disregarded and there had been a gross failure of the international community to enforce the protection which civilians deserved. Failure to observe this principle had led to severe suffering by the civilians.[54] It is clear that militaries are far too willing to disregard the law and this results in the reality that the law provides no protection for civilians. We can remain hopeful, however that in the future these principles will be adhered to.

The future of the principle of distinction

[48] Security Council Resolution 713 25 September 1991.

[49] The arms embargo can be viewed as illegal as the Bosnian government was prevented from using its right to self-defence of Article 51 United Nations Charter. *See* Procida "Ethnic cleansing in Bosnia-Herzegovina, a case study: employing United Nation mechanisms to enforce the convention on the prevention and punishment of the crime of genocide" 1995 *Suffolk Transnat'l L. Rev.* 655 678 fn 116.

[50] Procida "Ethnic cleansing in Bosnia-Herzegovina, a case study: employing United Nation mechanisms to enforce the convention on the prevention and punishment of the crime of genocide" 1995 *Suffolk Transnat'l L. Rev.* 655 670.

[51] The Serbs attacked a "safe zone" civilian market place in Sarajevo killing 68 people. NATO demanded that Serbs remove their artillery around Sarajevo but enforcing the demand required thousands of troops which the U.N. had failed to provide. *See* Procida "Ethnic cleansing in Bosnia-Herzegovina, a case study: employing United Nation mechanisms to enforce the convention on the prevention and punishment of the crime of genocide" 1995 *Suffolk Transnat'l L. Rev.* 655 677 fn 114.

[52] Olson, Cassel, Fielding, Burkhalter "Bosnia, war crimes and humanitarian intervention" 1994 *Whittier L. Rev.* 445 446.

[53] Security Council resolution 1031 15 December 1995.

[54] *Mothers of Srebrenica v The State of the Netherlands and the United Nations* Court of Appeal The Hague case number 200.022.151/01, judgment delivered 30 March 2010.
Case concerning the application of the convention on the prevention and punishment of the crime of genocide (Bosnia and Herzegovina v Serbia and Montenegro) ICJ General List no. 91 judgment delivered 26 February 2007.

International law's provisions of rights through distinction are nothing if not observed. Insurgencies occur against civilians without consideration for international law.[55] The principle of distinction is honourable but it is not effective in reality. It is essential to the confidence in humanitarian law that something be done to ensure effective protection of civilians in modern wars. Does the solution lie in a change to the principle itself or more broadly in observance of international law as a whole?

Swiney suggests that distinction be completely replaced.[56] His main arguments are that insurgents sometimes have legitimate reasons to disregard protection of civilians and that not all civilians should be protected equally. His solution is to replace distinction with the principle of culpability which provides that "it is impermissible to intentionally attack civilians or civilian objects unless the target voluntarily a) enters or remains in a contested area or area of combat and b) performs actions intended to achieve military goals of the combatants."[57] Distinction groups together all civilians whereas culpability individualises each civilian's role in the conflict. Voluntariness is required as it wouldn't be justified to target a civilian who has been forced by a party to the conflict to participate therein. As civilians are often used in the industrial side of military operations, the first requirement limits the involvement of civilians to be those in the area of combat so as not to stretch the limitation on protection further than it ought to. Performing actions intended to achieve military goals limits the protection afforded to civilians who have made the choice of taking part in the conflict.[58] A civilian cannot be separated from the military where he performs a military objective. This also prevents the stronger power from shielding itself from weaker parties to the conflict by making use of civilian contractors. Attacks against civilian settlers used for a military purpose of occupying territory would thus be permissible. Civilian contractors would also be legitimate targets. Culpability would favour weaker parties to conflict in the way that distinction favoured stronger ones. Swiney is hopeful that this change would encourage adhearance to the laws of war as it would be favourable to insurgents where distinction was not.

---

[55] Example Iraq, Israel, Palestine and Sri Lanka. Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 737.
[56] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 756.
[57] Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733 757.
[58] Civilian journalists or aid workers in the area of conflict, for example, would not have limited protection as they had no intention of becoming part of the conflict.

Von Sternberg's solution is somewhat different. He believes the issue must be solved through individual responsibility and prosecution.[59] Repetitive non-compliance with international law has resulted in unwanted violence during armed conflict and eroded respect for in international humanitarian law. This cannot be permitted to continue. According to him, violation of *jus cogens* norms such as those of Common Article 3 and the fundamental principles of Protocol II give rise to universal jurisdiction and States and tribunals have an obligation *egra omnes* to bring violators to justice.[60] He suggests that ensuing peace will be vulnerable if public injustice is experienced and criminal acts of the past are tolerated. A commitment to humanitarian ideals and respect for the principle of distinction must be of utmost importance if one truly aims to establish peace within the state.[61] These may not be abandoned in times of conflict but must always be observed.[62]

According to Procida, a more effective, immediate solution of ensuring that civilians are protected from attack is needed. A tribunal prosecuting violators of international law is ineffective in ending genocide as its authority is limited *ex post facto*. In the ongoing genocides of Bosnia, restraining of military aggression was far more necessary than adjudicating individual cases. The decision against providing collective security measures from the outset suggests that Council members must have a political interest in the situation before consenting to the action.[63] She foresees a solution in establishing a United Nations standing army as required by its Charter.[64] In so doing U.N. military operations would bypass any national politics and expedite proceedings to end aggression against protected persons.[65]

While I agree there is an obvious deficiency in the adherence of distinction, I do not believe that the answer lies in replacing it with culpability. It is a longstanding and

---

[59] Von Sternberg "Yugoslavian war crimes and the search for a new humanitarian order: the case of Dusko Tadic" 1996 *St. John's J. Legal Comment* 351 375.
[60] Von Sternberg "Yugoslavian war crimes and the search for a new humanitarian order: the case of Dusko Tadic" 1996 *St. John's J. Legal Comment* 351 377.
[61] Von Sternberg "Yugoslavian war crimes and the search for a new humanitarian order: the case of Dusko Tadic" 1996 *St. John's J. Legal Comment* 351 375.
[62] Von Sternberg "Yugoslavian war crimes and the search for a new humanitarian order: the case of Dusko Tadic" 1996 *St. John's J. Legal Comment* 351 384.
[63] *Eg* United States interest in Somalia. Olson, Cassel, Fielding, Burkhalter "Bosnia, war crimes and humanitarian intervention" 1994 *Whittier L. Rev.* 445 458.
[64] Article 43.
[65] Procida "Ethnic cleansing in Bosnia-Herzegovina, a case study: employing United Nation mechanisms to enforce the convention on the prevention and punishment of the crime of genocide" 1995 *Suffolk Transnat'l L. Rev.* 655 685.

important principle of international law, entrenched in both customary and conventional law and serves an important purpose. To create a distinction between civilians would water down the protection they deserve. Contractors and settlers experience difficult circumstances during conflict and their motives are mainly of survival which is all the more reason to protect them. Individual prosecution of violators serves an important function as a deterrent to future violations of international law and affords peace to emerging democracies. The solution to the failure of the principle of distinction is "a climate of compliance."[66] This cannot be left to the law and judicial system alone but should incorporate public consensus. It would mean that government and non-government actors would observe international law. Until such a climate exists, however, the most immediate and effective solution to non-compliance is intervention. States should not place political interest before protected groups and should intervene at the first sign of atrocities being committed.

Conclusion

The principle of distinction is well entrenched in international humanitarian law and should continue to be observed throughout any means of armed conflict whether in the past, present or future. The principle, aiming to protect civilians, is not to be replaced but rather observed more consciously by all state and non-state actors. To consider its application and effectiveness in cyber warfare, however, it will first be necessary to determine the perimeters of the realm this method of warfare which will follow in Chapter Two.

[66] Meron "The humanization of humanitarian law" (2000) *American Journal of International Law* 239 277.

Chapter 2: Cyber warfare

At the time that the Hague and Geneva conventions were drafted the thought of cyber war constituted little more than science fiction.[67] The international conventions that regulate the law of war were designed in response to kinetic, and not cyber, technologies.[68] As Gervais so aptly put it, "[c]yberspace has become a new battleground for warfare."[69] The use of cyber weapons is therefore neither expressly regulated nor outlawed by international humanitarian law and the international community is divided on whether the rules of IHL should apply.[70] Today computers play a vital role in all aspects of civilian and military life such as communication, healthcare and power systems that some scholars have identified the need for a convention to be drafted on cyber laws. Others have noted that the rapid growth of cyber development will render the regulations obsolete "before the ink would be dry."[71] This analysis advocates the application of IHL to cyber war and to evolve traditional principles to apply thereto. In order to apply IHL to cyber war, however, it is first necessary to have a thorough understanding of this type of warfare.

Defining cyber war

"Cyberspace" comprises of the sum of electronic networks and information operations.[72] It is defined by the United States Military Strategy for Cyberspace Operations as "[*sic*] a domain characterized by the use of electronics and electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures".[73] This domain thus includes

---

[67] Brunner *The Shockwave Rider* (1975). This novel described a computer worm which was used to alter government data.
[68] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 526.
[69] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 526.
[70] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1430.
[71] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1430. *Also* Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 538.
[72] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 307.
[73] The National Military Strategy for Cyberspace Operations, December 2006, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf [accessed 16 December 2013 at 06:43].

information technology infrastructures such as the internet, telecommunications networks, computer systems as well as embedded processors and controllers.[74]

"Cyber attacks" are defined by the U.S. Army's Cyber Operations and Cyber Terrorism Handbook as the threat or premeditated use of disruptive activities against computer networks with the intention of causing harm or to further social, ideological, religious, political objectives which could harm computer networks, physical facilities and persons.[75] These attacks involve acts which aim to alter, disrupt, deceive, degrade or destroy adversary computer systems or networks or the information within these systems or networks.[76]

Cyber attacks are also defined by the Council of Europe's Convention on Cybercrime as those actions involving the damaging, deletion, deterioration, alteration or suppression of computer data without right and those seriously hindering the right of functioning of a computer system by similar means.[77] These attacks are hostile acts which can be isolated acts, initiate armed conflict or may be a reaction to a prior conventional or cyber attack.[78]

Cyber weapons are defined by the Tallinn Manual as any cyber device, material, instrument, mechanism, equipment or software used, designed or intended to be used to conduct a cyber attack.[79] It can take various forms including syntactic, semantic and mixed weapons.[80] Syntactic weapons target operating systems through the use of malicious code in viruses, worms, Trojan Horses, distributed denial of service attacks (DDoS) and spyware.[81] Semantic weapons attack the accuracy of data contained by the computer, for example, by altering data to produce errors without the user having knowledge as to this alteration or errors.[82] Mixed weapons combine use of syntactic and semantic weapons to attack both the

[74] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 86.
[75] US Army Training & Doctrine Command, DCSINT Handbook no. 1.02, Critical infrastructure threats and terrorism at VII-2, 15 August 2005.
[76] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 533.
[77] Council of Europe, Convention on Cybercrime *opened for signature* 23 November 2001 Article 5.
[78] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 96.
[79] Tallinn Manual on the International Law applicable to Cyber Warfare (Schmitt, gen. ed., forthcoming Cambridge University Press 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 [last accessed: 16 December 2013 at 07:22]. Rule 41.
[80] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 537.
[81] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 310.
[82] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 311.

operating system and the data which it contains resulting in a more sophisticated weapon.[83] Effects of such attacks could range from simple inconvenience, for example by way of a DDoS attack which disrupts web traffic temporarily, to physical destruction for example by altering instructions which causes a power generator to explode, to death for example by disrupting access to emergency services.[84] One can herein understand why American President Barack Obama eloquently described such weapons as "weapon[s] of mass *disruption* [own emphasis]."[85]

It is to be here noted that "cyber crimes" are distinct from cyber attacks as these involve crimes regulated by domestic law such as internet fraud and as such will not be discussed any further. "Cyber exploitation" consists of deliberate action aiming to extract confidential information from an adversary's computer system or network without the user's knowledge and as a result, amounts to espionage.[86] This may well be criminalised by domestic laws but is not prohibited by international law.[87]

Positive aspects of cyber war

As states advance in their development of technology, they are increasingly vulnerable to cyber attacks. States such as America have accepted that their economy and national security have become fully dependent on information technology.[88] This is relevant in that both civilians and militaries rely on technology and an attack thereof could paralyse a state in its entirety. In recent history we have seen a shift from individual "hackers" with the intention of personal gain through their crimes (for example theft through online banking) to state or terrorist organisations making use of cyber war to further their political aims and agendas.[89] This form of warfare is a lot faster than traditional concepts of war as geographical distance is irrelevant and targets may be reached from across the globe within seconds.[90]

---

[83] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 311.
[84] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 537.
[85] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 109.
[86] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 533.
[87] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 533.
[88] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 87.
[89] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 87.
[90] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 87.

The use of cyber warfare and weapons is appealing as it may result in fewer civilian deaths than the use of traditional kinetic weapons.[91] This is a result of the ability to reach targets with precision without causing civilian casualties.[92] This warfare is also much cheaper than traditional warfare due to the low cost and wide availability of computers.[93] The fact that this method of war is cheaper than traditional arsenals used for war is favourable to weaker states or non-state actors which cannot afford sophisticated weapons but are able to use cyber weapons to create the same consequences.[94] Such consequences could include disabling power generators, damage nuclear reactors, derail trains, open dam walls or explode pipelines.[95]

Cyber attacks are also viewed favourably by attackers due to the fact that one can conduct them anonymously as it is difficult to determine who is responsible for such attacks.[96] This is due to technicalities such as IP spoofing or use of botnets which create the appearance of attacks originating from one state while in fact originating from another.[97]

The potential harm to be created by cyber war has resulted in some states such as the United States designating cyber threats as the greatest danger to national security second only to nuclear weapons.[98] Russia considers this threat of such severity that it has reserved the right to use nuclear weapons to counter a cyber attack.[99] It can thus be established that governments recognise the severity of the potential outcome of such attacks.

Instances of cyber warfare

To allow an analysis of the role of traditional principles of IHL such as that of distinction in the realm of cyber war, it is necessary to consider particular

---

[91] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1438.
[92] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 846.
[93] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 304.
[94] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 87.
[95] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 88.
[96] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 304.
[97] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 96.
[98] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 846.
[99] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 846.

occurrences of cyber warfare. While there are various instances to examine, this analysis will limit discussion to those acts experienced by Georgia, Estonia and Iran.

A. Georgia

In 2008 war broke out between Russia and Georgia over the territory of South Ossetia which was a pro-Russian area of Georgia.[100] Traditional methods of war were used as Tbilisi, Georgia's capital, was bombed by Russian bombers. These bombs targeted Georgia's economic infrastructure by means of damaging their largest port and main roads.[101] These hostilities triggered the laws of international armed conflict and IHL.

Georgia also experienced attacks on its internet infrastructure though defacement and denial of service operations on the cyber front including targets such as the websites of the President, Parliament, Foreign Affairs, Defence and Education ministries, domestic and foreign media, banks and private internet servers.[102] The Minister of Foreign Affair's website was defaced with pictures of Adolf Hilter together with Georgia's president, Mikheil Saakashvili. Georgia's National Bank website was replaced with one of dictators of the twentieth-century together with Georgia's president. Each operated for an average of two hours and no physical damage or injuries were reported as a result of these operations. Services, however, were seriously disrupted.[103] The Georgian government was rendered unable to transmit information about the situation. Banking was brought to a halt as banks went off-line. Mass confusion was experienced in Georgia as communication was hindered.

The attackers used a method termed DDoS which bombards a website with millions of requests in order to overload its server which then shuts it down.[104] These operations were traceable to Russia but no clear evidence could be found to identify

[100] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303.
[101] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303.
[102] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89.
[103] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89.
[104] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 304.

the Russian government as being responsible even though government computers were used in certain circumstances to conduct the attacks.[105]

In order to alleviate the disruption to some extent, Google provided hosting for various websites, government websites of the Ministry of Defence and Ministry of Foreign Affairs were moved to American and Estonian servers and the Polish President's website was made available to the Georgian government to provide information about the conflict.[106] Although these methods of assistance were certainly helpful, the operations severely impacted Georgian cyber infrastructure.[107]

It should be noted that this cyber attack was probably the first time this method of attack was used in conjunction with traditional kinetic methods of military action which illustrates the way in which the methods of war are changing.[108] This particular operation evidences the fact that states are attracted to engage in cyber attacks to weaken opponents' critical infrastructures such as national and economic security, public health and safety which provides them with military advantage during conflict.

B. Estonia

Members of the Soviet Union built a bronze memorial statue in Tallinn, the capital of Estonia. This statue was largely viewed as a reminder of Soviet occupation and repression during World War II although citizens of Russian decent viewed the statue as a tribute to Soviet soldiers lost in the war. Due to its controversy, it was decided that the statue would be removed in 2007. This decision was followed by two nights of riots termed "Bronze Night."[109]

Estonia suffered serious cyber attacks following Bronze Night which severely affected its digital infrastructure.[110] These attacks originated mainly from Russia.[111] These cyber attacks lasted the duration of three weeks, first affecting government websites and then moving on to affect newspapers, television stations, banks and

[105] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 90.
[106] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 90.
[107] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 90.
[108] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 304.
[109] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 539.
[110] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 539.
[111] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 540.

other targets.[112] The consequence of such attacks was more than mass confusion of the public as crucial government and commercial websites were targeted but emergency services were also brought to a halt.[113] The phone numbers for ambulances and fire brigades were rendered ineffective for over an hour, endangering lives, which was seriously problematic at a time of serious public unrest and riots. As a result, 150 people were injured and one death occurred.[114]

C. Iran

In 2010 Iran experienced a cyber attack that was discovered by a technical security firm in Belarus.[115] The attack took the form of malware called "Stuxnet."[116] This malware was able to hack the Windows operating system as well as target Iran's nuclear weapons facility.[117] It is suspected that Israel and the United States were behind this attack which aimed to destroy the uranium enrichment centrifuges at Iran's Natanz nuclear facility.[118] This attack resulted in Iran's nuclear program being set back several years although Iran officials initially denied that any damage was sustained. President Mahmoud Ahmadinejad declared that Stuxnet had caused damage to a limited number of centrifuges but evidence suggests that significant damage did in fact occur as inspections have found that close to 1000 centrifuges were removed from Natanz.[119]

Stuxnet had two main technical functions. The first was to rapidly increase or decrease the speed at which the rotations of centrifuges occurred which would result in their destruction. The second was to alter the messages sent to the facility's operators indicating that the centrifuges were working normally. The operators are

---

[112] Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85 89.
[113] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 309.
[114] Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303 310.
[115] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 843.
[116] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 843.
[117] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 843.
[118] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 844.
[119] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 844 and 858.

thus unaware of the problems and unable to prevent the destruction of the centrifuges.[120] It was therefore able to hide it from any form of detection.

Stuxnet has been described as a "remarkable piece of malware" and the reasons for such can be described as follows.[121] The code runs according to four main questions: 1) determining whether it is running within a Supervisory Control and Data Acquisition software control system; 2) if yes, whether it is running Siemens (who is the manufacturer of the Iranian plant controls); 3) if yes, whether it is running Siemens 7 (a category of software control systems); 4) if yes, whether the software is contacting an electrical motor designed by one of these companies.[122] If answered in the affirmative, the only possible target is Natanz.

Stuxnet therefore comprises of unprecedented precision in seeking its target comparable to kinetic technology of stealth drones.[123] As a result of its precision, it has the ability to limit the destruction it creates unlike other traditional kinetic weapons which gives reason to the fact that it is considered a major development in warfare.[124] It struck only the centrifuges without affecting any civilian workers at the facility or any civilian computer systems which is remarkable. This is especially the case if one compares this attack to the 2007 Israeli bombing of a Syrian facility suspected of functioning as a nuclear reactor which had such widespread effects that it left only "a big hole in the desert."[125]

The level of sophistication of Stuxnet leads analysts to believe that it could only have been possible to create with five to ten programmers working for a duration of six

[120] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 844.
[121] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 852.
[122] Rosenbaum "Richard Clarke on who was behind the Stuxnet attack" http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html?c=y&page=3 [accessed 8 July 2013 at 21:27].
[123] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 852.
[124] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 852.
[125] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 860.

months.[126] Evidence suggests that the programmers were well-financed and organised.

There is no concrete evidence to confirm that the attack was directed by Israel and the United States which clearly illustrates the anonymity that follows cyber war. Neither state has confirmed nor denied responsibility however there is political cause suggesting that these states were involved in the attack.[127]

Conclusion

It can be seen through the use of definitions on the topic as well as practical scenarios as evidenced in Georgia, Estonia and Iran that cyber war is a highly technical realm of warfare. It has various differences to kinetic methods of war and these may be used to the advantage of States as they have the ability of being far more precise in reaching their targets. International humanitarian law applies to all armed conflict and as such there exists the possibility of ensuring greater observance to the principle of distinction through this method of warfare. This possibility will now be analysed in the following chapter.

[126] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 855.
[127] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 845.

Chapter 3: Applicability of IHL to cyber attacks

International humanitarian law aims to alleviate the calamities of war by implementing limitations of conduct by states party to armed conflict. Gervais states that these customary law limitations are not contingent on the type of weapons used and are thus applicable to cyber attacks regardless of the fact that it is a relatively new method of warfare.[128] As militaries increasingly use cyber operations in warfare, the principle may need to be reinterpreted to be effectively applied.[129] For the most part, however, anything considered a legitimate target in a conventional attack would be a legitimate target for a cyber attack.[130]

The International Strategy for Cyberspace issued by the United States stated that customary international law need not be reinvented to enable it to apply to state conduct in cyberspace.[131] It states that these norms are not obsolete but are in fact applicable to cyber warfare however there are unique characteristics to cyber warfare which require additional regulations to clarify exactly how these rules apply.[132]

The most recent developments in providing supplementary sources of regulations on the topic are that of the speech given by Harold Koh at the conference sponsored by the United States Cyber Command (USCYBERCOM) as well as the Tallinn Manual (2013) written by NATO's Cooperative Cyber Defence Centre of Excellence, in particular, the International Group of Experts.[133] The Tallinn Manual it was drafted by the most distinguished of legal academics, practitioners and technical experts while USCYBERCOM, the ICRC and NATO participated as observers in the

---

[128] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 563.
[129] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1437.
[130] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1437.
[131] The White House, International Strategy for Cyberspace: prosperity, security and openness in a networked world 9 (2011) *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [last accessed: 16 December 2013 at 07:32].
[132] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 14.
[133] Harold Honhgu Koh, Legal Advisor of the Department of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (18 September 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm [last accessed: 16 December 2013 at 07:42].

process.[134] There is a tremendous amount of congruency these two sources which is indicative of *opinio juris*.[135]

On the applicability of international law to cyber attacks, these sources consider the International Court of Justice's decision taken in the *Nuclear Weapons* Advisory Opinion.[136] The court held that the prohibition of the use of force found in Article 2(4) of the United Nations Charter applied to use of nuclear weapons.[137] It was found that the prohibition applied to any use of force regardless of the weapons used.[138] The Experts are thus of the opinion that where computers are used as weapons in an operation this will have no effect on the fact that the use of force is prohibited. The court also considered IHL which it held that belligerents are not unlimited in the means which they use to attack the enemy.[139] It considered the principles of distinction and unnecessary suffering as a foundation for analysing the legality of use of nuclear weapons.[140] From this Experts deduced that IHL principles apply to nuclear weapons regardless of the fact that they predate the use thereof and found no reason why they should not be applicable to cyber weapons.[141]

Of further relevance is that the court and Experts considered the Martens Clause, first contained in the preamble of the Hague Conventions and later the Geneva Conventions, which states that in circumstances which are not covered by international agreements, "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[142] While there may exist *lacuna* of directly applicable cyber treaty law, this does not create a situation free from international humanitarian law, but rather suggests that cyber

---

[134] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 15.
[135] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 15.
[136] *Legality of the threat of use of nuclear weapons* Advisory Opinion, 1996 ICJ 226 (hereinafter, Nuclear Weapons).
[137] Charter of the United Nations *signed on* 26 June 1945, article 2, par. 4; article 51; article 42.
[138] *Nuclear Weapons* par 39.
[139] *Nuclear Weapons* par 77.
[140] *Nuclear Weapons* par 78.
[141] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 17.
[142] Convention (II) with respect to the Laws and Customs of War on Land, preamble, *signed on* 29 July 1899. Protocol Additional I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I) *signed on* 8 June 1977, article 1(2).

weapons are subject to pre-existing law.[143] At the heart of this application lies the principle of distinction.

The Principle of Distinction

As stated in chapter 1, this principle requires attackers to distinguish between civilians and combatants as well as civilian objects and military objectives.[144] Civilians enjoy a general protection from the dangers of military operations and are not to be the targets of or suffer as a result of any indiscriminate attack.[145] This principle provides that only combatants and military objectives serve as legitimate targets in warfare. The International Court of Justice has labelled distinction as one of two cardinal principles of international humanitarian law.[146] Failure to adhere to this principle would constitute a war crime.[147]

An attack may not have the effect of destroying anything of essential value to the survival of the civilian population such as food, crops, livestock, water, etc.[148] States are also prevented from using any weapon that is incapable of distinguishing between civilian and military targets.[149] Combatants have a duty to minimize civilian deaths and damage to civilian objects. This requires combatants to launch attacks only against objects that make an effective contribution to military action which would offer a definite military advantage.[150]

The principle of distinction requires military commanders to anticipate the consequences of their attacks. Kelsey considers the hypothetical situation of conducting a cyber attack which neutralises an air defence station which would

[143] Article 36 Geneva Convention Additional Protocol I. Tallinn Manual on the International Law applicable to Cyber Warfare (Schmitt, gen. ed., forthcoming Cambridge University Press 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 [last accessed: 16 December 2013 at 07:22], Rule 48.
[144] Article 48 Geneva Convention Additional Protocol I.
[145] Article 51 Geneva Convention Additional Protocol I.
[146] *Nuclear Weapons* par 78. The other principle is the prohibition of unnecessary suffering.
[147] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 565.
[148] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1436.
[149] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1436.
[150] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1437.

provide military advantage. A cyber attack of such a station could result in fewer civilian deaths than a conventional attack and as such it would seem a legitimate attack. If, however, such attack indirectly resulted in false messages being sent to an air-defence network which as a consequence endangers relief or commercial air traffic, the consequences of such attack may threaten the lives of civilians which would be impermissible regardless of the military advantage attained.[151] The principle applies equally in situations where a cyber attack is directly intended to cause civilian death or injury such as targeting an air traffic control tower which causes civilian aircrafts to crash or disrupting databases which results in wounded soldiers receiving blood transfusions of the incorrect blood type. Such scenarios do not provide military advantage and only cause harm to civilians which would require military leaders to forgo such attacks.[152]

While it has been stated that this general principle is applicable to the realm of cyber warfare, this does not occur without complications. Civilian infrastructure is often used in cyber attacks to conduct military operations and this fact blurs the lines of distinction.[153] It must thus be established whether the attack can sufficiently distinguish between civilian and military targets as well as whether the attack occurs indiscriminately without consideration for civilian population.[154]

Problematic application of distinction

For the most part, the application of international humanitarian law principles will raise the same controversies as those raised in attacks on land, sea and in the air as generally stated in Chapter 1, however there are some that are unique to cyber warfare.[155]

A. Civilians taking direct participation in hostilities

[151] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1438.
[152] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1438.
[153] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 565.
[154] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 565.
[155] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 17.

Combatants may be defined as organised armed forces, groups or units under the command of the state.[156] They are required to distinguish themselves from the civilian population for the duration that they are involved in or are preparing to be involved in armed conflict. Non-combatants comprise of civilians and enemy personnel out of combat.[157]

The requirement of organisation is applicable to states with armed forces that have the capabilities of conducting cyber attacks. It is however problematic in the situation when unorganised, individual "hackers" conduct attacks as acts of ideology or patriotism as it raises the question whether the state which has been targeted may retaliate with proportional force.[158] It is obvious that this individual hacktivist is not considered a combatant. The hacktivist would thus be considered a civilian taking direct part in hostilities and thus would not be afforded the protection of other civilians not taking direct part therein.[159] The hacktivist would be a valid target only for the duration of which he participates in hostilities.

This is further problematic as there is often a gap in time that exists between the attack being launched and its detection or discovery of its source.[160] If a hacktivist is a legitimate target only for the duration that he is involved in such attack, he may have reverted back to the protection afforded to civilians not taking direct part in hostilities, as a result of the gap in time, when the source of the attack is discovered. This would mean that the targeted state may not implement a counterattack against the hacktivist.[161]

Gervais states that in this type of scenario it may be suitable to shift responsibility to states by requiring states to prohibit, prevent or stop cyber attacks from originating on their internet infrastructure.[162]

B. Dual-use objects

[156] Article 43 Geneva Conventions Additional Protocol 1.
[157] Article 50(1) Geneva Convention Additional Protocol 1.
[158] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 566.
[159] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 566.
[160] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 566.
[161] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 566.
[162] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 566.

A further problematic scenario with the principle of distinction in cyber warfare presents itself in the form of dual-use objects. In cyber operations this would mean that the cyber infrastructure is shared by the military and civilians.[163]

The Koh speech it was stated that dual-use infrastructure raises questions as to the rule of proportionality and the rule prohibiting the use of civilian objects to shield military objectives from attack.[164] Civilian cyber infrastructure would be needed to shield military operations. This prohibition, according to Schmitt with use of the weak interpretation of distinction, becomes moot where objects such as computers, computer networks and cyber infrastructure are used for both civilian and military purposes as this then becomes a military objective and thus a valid target.[165]

The principle of proportionality will be taken into consideration where civilians or civilian objects have been affected following an attack on dual-use cyber infrastructure.[166] Problematic situations exist here as it is often difficult to determine which parts of the dual-use object was used for military transmissions and as such this could render an entire network a military objective. Social networks such as Twitter, Facebook and other social media have been used to transmit military information in recent conflicts and the Experts agreed that this would render those areas of social media networks military objectives however it would not be acceptable to subject the entire network to attack.[167]

It is possible with this method of warfare that a civilian computer could be hijacked for the purpose of conducting a military attack. Gervais provides that such an instance would involve two violations.[168] Firstly, the civilian computer would have been unlawfully breached by the attacker in order for him to conduct the attack. The targeted state would then retaliate against the civilian computer causing collateral

---

[163] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 29.
[164] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 29.
[165] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 29.
[166] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 29.
[167] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 30.
[168] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 567.

damage to civilian objectives. Here the attacker would be responsible for damage caused to the civilian property.[169]

Secondly, this would result in a civilian unwillingly entering into hostilities which is prohibited by the Geneva Conventions. A situation comparable to that of human shields would be created in which, as a civilian object, the computer should be protected from attack even though it was used for a military attack against another state.[170]

C. Nonlethal Potential

Kelsey recognises that the nonlethal potential of cyber weapons may cause more frequent violations of the principle of distinction which could cause the erosion thereof.[171] Cyber weapons are able to provide a military advantage without the threat of civilian lives which conventional attacks would produce and this could lead to belligerents to disregard the principle which IHL aimed to protect.[172]

To illustrate this aspect he considers the NATO bombing of Serbian media station RTS during the armed conflict in Kosovo. NATO provided that the reason for such an attack was to prevent Serbian propaganda and military communications and as such considered RTS a legitimate military target. NATO has been criticised for such an attack which provided relatively little military advantage when weighed against the loss of sixteen civilian lives. Had a cyber attack been used instead of conventional bombing, the death of civilians may have been completely avoided. The question military advantage would still remain as the media station was a predominantly civilian object, however the military communication would have been eliminated.[173]

The principle of distinction, it would seem, is less likely to be considered in less severe scenarios which are unaccompanied by civilian death and Kelsey notes that

---

[169] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 567.
[170] Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 567.
[171] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1439.
[172] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1430.
[173] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1440.

belligerents may apply this logic to their favour.[174] Cyber attacks have the capability of neutralising targets without causing physical damage unlike conventional attacks and this fact could cause an influx in the use of cyber weapons against conventionally protected civilian objects which should be protected from attack.[175]

On this observation Greenberg notes that it is unclear whether attacks which result in disruption of financial or social security systems, disclosure of confidential information or other intangible consequences fall into the category of injury which international humanitarian law aims to prevent.[176]

D. Cyber operations do not necessarily equate to cyber attacks

Principle of distinction requires the protection of civilians during military operations.[177] Schmitt emphasises that these military operations must consist of an attack.[178] He finds that certain kinds of operations such as psychological operations do not amount to attacks and as a result these operations would be lawful.[179] For a military operation to amount to an attack, it must consist of an act of violence against an adversary whether in offence or defence.[180]

If one follows a strict interpretation this would mean that non-kinetic operations (not comprising of a physical force) would not be considered attacks. As a result operations not involving acts of violence or physical force such as propaganda, embargoes or other psychological or economic warfare would not be considered attacks. This interpretation is supported by the International Red Cross *Commentary* on Article 49 which suggests that an attack comprises of combat in action.[181]

At the time in which the Geneva Conventions were drafted attacks were mainly kinetic and cyber operations were unheard of. If one considers this fact in context,

---

[174] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1440.
[175] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1440.
[176] Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427 1441.
[177] Article 57(1) Geneva Convention Additional Protocol 1.
[178] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 92.
[179] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 92.
[180] Article 49 Geneva Convention Additional Protocol 1.
[181] International Committee of the Red Cross, Commentary on the Additional Protocol of 8 June 1977 to the Geneva Conventions of 12 August 1949.

violence can be viewed as a useful indication of attacks where civilians were to be protected. Schmitt states that while these rules appear to be act-based, they are in fact consequence-based.[182] He finds evidence as to this conclusion in the treaty's protection from danger of injury or loss of civilian life or damage to civilian objects.[183] It is thus not the violence of the act but the violence of the end result of such act which determines its limitation.[184]

Through this interpretation we can determine that biological, chemical and cyber operations can generate circumstances with violent consequences and as such amount to attacks even though no physical force was used.[185] Further support for this view can be found in the Tallinn Manual which states that while cyber operations may be non-violent as a result of not releasing kinetic energy, the may have violent consequences such as death, damage, injury or destruction.[186] An example of such non-violent acts would be if one attacks an air traffic control tower, as considered above, which would have violent consequences for civilian aircraft. Relevant here would be the cyber operations which affected Georgia. If one follows the above interpretation, the disruption and defacement that was experienced did not amount to any physical harm, damage or injury and thus could not be described as "attacks" but merely inconvenience. As a result, these operations are insufficient to be rendered unlawful by IHL.[187]

Dörmann advocates a different perspective focusing on the definition of military objectives.[188] These are limited to objects "[*sic*] which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[189] By the inclusion of neutralisation one need not consider the stronger requirements of damage, destruction, death or injury to

---

[182] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 93.
[183] Article 51 and 57.
[184] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 94.
[185] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 94.
[186] Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13 26.
[187] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 95. Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525 568.
[188] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 95.
[189] Article 52(2).

qualify as an attack.[190] Under this interpretation, cyber operations targeting civilians is prohibited regardless of the consequence of such an attack. In this regard the cyber operations which affected Georgia's infrastructure would qualify as a prohibited attack against civilians.[191]

The first approach may be seen as under-inclusive in that it does not regulate disruptive activities as experienced by Georgia but Dörmann's approach is over-inclusive. By including mere inconvenience into the definition of an attack one would be stretching the principles of IHL further than intended. It is clear that uncertainty exists as to where distinction lies. Some situations, however, establish the line of distinction with relative ease.

Stuxnet: a perfect fit

Richard Clarke, former United States counterterrorism czar, aptly described Stuxnet's code in the following manner: "it just says lawyers all over it."[192] The manner in which this cyber attack fits to the form of IHL is indicative that the programmers behind it received legal advice from international lawyers.

Had Natanz not been a valid military objective, Stuxnet would be illegal. Instead it was a legal target under the principle of distinction for the following reasons. There exist two possible reasons for the purpose of enriching uranium at this plant. The first being the potential of creating a nuclear weapon which immediately identifies Natanz as a military objective. The second would be to fuel nuclear power plants which would enable it to power military structures. By providing electricity to military operations, Natanz would be providing a military contribution and, by disrupting the generation of such power would provide military advantage to belligerents. According to Richmond, "a facility that provides essential component parts to power plants – here the enriched uranium – also would be a valid military objective".[193]

He is if of the opinion that had Stuxnet intentionally infected civilian computers to advance itself to infecting Natanz, this may have lead to the violation of distinction,

---

[190] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 95.
[191] Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89 95.
[192] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 857.
[193] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 884.

even where no harm was suffered. This would have been the case where Stuxnet specifically targeted these computers which would then violate the principle.[194]

The fact that Stuxnet's code is so specific in determining its target lowers the lever of destruction and allows the belligerents to target on the military objective being Natanz. With its precision it decreases the harm which may have been suffered by civilians had another (kinetic) weapon been used. Stuxnet therefore adheres to the principles of distinction and as such constituted a lawful attack in terms of IHL.[195]

It is thus possible that a cyber attack may be conducted in a way that meets the requirements of international humanitarian law and as such fits the perimeters for which IHL was intended. As analysed, however, this is a new development in wafare and as such not every aspect of this method of war is covered and uncertainty exists over acts which may be viewed as aggression however fall below the threshold required to exist as armed conflict.

Conclusion

International humanitarian law is to be observed with utmost importance during all methods of warfare. Weapons will continue to advance, develop and become more sophisticated at a rapid pace but, as this analysis has evidenced, the foundational principles of this branch of law will not change. The principle of distinction lies at the core of international humanitarian law and exists to protect civilians from the terrors of war. This principle must continue to be observed throughout time regardless of the development in attacks.

The principle of distinction does not exist without uncertainties. Cyber warfare, most part, experiences the same uncertainties as those that exist in the realm of kinetic warfare. The fact that various uncertainties exist around cyber warfare is not in itself enough to relinquish this method of warfare from international humanitarian law and as a result the principle of distinction. While there are certain grey areas unique to cyber war, these may be clarified through the drafting of supplementary regulation in

[194] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 885.
[195] Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842 885.

the future. For now, however, the laws that have existed in times where only traditional kinetic warfare was imagine are adequate to apply in this new field of war. As such, it may be said that the principle of distinction is in fact effective in light of cyber warfare.

Bibliography

Articles

1. Swiney "Saving lives: the principle of distinction and the realities of modern war" 2005 *INT'L Law* 733
2. Procida "Ethnic cleansing in Bosnia-Herzegovina, a case study: employing United Nation mechanisms to enforce the convention on the prevention and punishment of the crime of genocide" 1995 *Suffolk Transnat'l L. Rev.* 655
3. Olson, Cassel, Fielding, Burkhalter "Bosnia, war crimes and humanitarian intervention" 1994 *Whittier L. Rev.* 445
4. Von Sternberg "Yugoslavian war crimes and the search for a new humanitarian order: the case of Dusko Tadic" 1996 *St. John's J. Legal Comment* 351
5. Meron "The humanization of humanitarian law" 2000 *American Journal of International Law* 239
6. Gervais "Cyber attacks and the laws of war" 2012 *Berkeley J. Int'l L.* 525
7. Kelsey "Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare" 2007 *Mich. L. Rev.* 1427
8. Swanson "The era of cyber warfare" 2010 *Loy. L.A. Int & Comp. L. Rev.* 303
9. Roscini "Wold wide warfare – Jus ad bellum and the use of cyber force" 2010 *Max Planck UNYB* 85
10. Schmitt "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" 2012 *Harvard International Law Journal* 13
11. Richmond "Evolving Battlefields: Does Stuxnet demonstrate a need for modifications to the law of armed conflict?" 2011 *Fordham Int'l L.J.* 842
12. Schmitt "Cyber Operations and the Jus in Bello: Key Issues" 2011 *Int'l L. Stud. Ser. US Naval War Col.* 89.

Books

1. Bassiouni *International Criminal Law: Sources, Subjects, and Contents* (3rd ed).
2. Thürer *International Humanitarian Law: theory, practice, context* (2011).

3. Henckaerts, Doswald-Beck *Customary international humanitarian law, Volume II: Practice* (2005
4. Crowe, Weston-Scheuber *Principles of International Humanitarian Law* (2013).
5. Cryer, Friman, Robinson, Wilmshurst *An introduction to international criminal law and procedure* (2007).
6. Aust *Handbook of International law* (second edition).
7. Cassese, Acquaviva, Fan and Whiting *International Criminal Law cases and commentary* (2011).
8. Brunner *The Shockwave Rider* (1975).

Case law

1. *Nicaragua v United States* 1986 ICJ 4 105.
2. *North Sea Continental Shelf* 1969 ICJ Reports 3.
3. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* 27 June 1986 ICJ Reports 14.
4. *Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, The Prosecutor v Dusko Tadic* Case No. IT-94-1-AR72 (International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed on the Territory of the Former Yugoslavia 1995).
5. *Prosecutor v Galic* Judgment Case No. IT-98-29-T ICTY Trial Chamber 5 December 2003.
6. *Prosecutor v. Kordic and Cerkez* Judgment Case No. IT-95-14/2-T ICTY Trial Chamber 26 February 2001.
7. *Mothers of Srebrenica v The State of the Netherlands and the United Nations* Court of Appeal The Hague case number 200.022.151/01, judgment delivered 30 March 2010.
8. *Case concerning the application of the convention on the prevention and punishment of the crime of genocide (Bosnia and Herzegovina v Serbia and Montenegro)* ICJ General List no. 91 judgment delivered 26 February 2007.

9. *Legality of the threat of use of nuclear weapons* Advisory Opinion, 1996 ICJ 226 (hereinafter, Nuclear Weapons).

Internet

1. Rosenbaum "Richard Clarke on who was behind the Stuxnet attack" http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html?c=y&page=3 [accessed 8 July 2013 at 21:27].

Treaty law

1. St. Petersburg Declaration 11 December 1868.
2. Convention (II) with respect to the Laws and Customs of War on Land, preamble, *signed on* 29 July 1899.
3. Convention (IV) respecting the Laws and Customs of War on Land *signed at* The Hague 18 October 1907.
4. Geneva Convention (III) Relative to the Treatment of Prisoners of War, 12 August 1949.
5. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) *opened for signature* 12 December 1977.
6. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
7. International Committee of the Red Cross, Commentary on the Additional Protocol of 8 June 1977 to the Geneva Conventions of 12 August 1949 636 (1987).
8. Vienna Convention on the Law of Treaties 22 May 1969.
9. The Convention on the Prevention and Punishment of the Crime of Genocide 9 December 1948.
10. The Laws of War on Land adopted by the Institute of International Law, Oxford, 9 September 1880.

11. Instructions for the Government of Armies of the United States in the Field, General Orders No. 100 (Lieber Code) 24 April 1963.
12. Council of Europe, Convention on Cybercrime *opened for signature* 23 November 2001.
13. Charter of the United Nations *signed on* 26 June 1945.

Military manuals

1. The National Military Strategy for Cyberspace Operations, December 2006, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf [accessed 16 December 2013 at 06:43].
2. US Army Training & Doctrine Command, DCSINT Handbook no. 1.02, Critical infrastructure threats and terrorism at VII-2, 15 August 2005.
3. United States Department of Air Force, USAF Intelligence Targeting Guide, February 1998.
4. Tallinn Manual on the International Law applicable to Cyber Warfare (Schmitt, gen. ed., forthcoming Cambridge University Press 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 [last accessed: 16 December 2013 at 07:22].
5. The White House, International Strategy for Cyberspace: prosperity, security and openness in a networked world 9 (2011) *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [last accessed: 16 December 2013 at 07:32].

Speech

1. Harold Honhgu Koh, Legal Advisor of the Department of State, International Law in Cyberspace, Address to the USCYBERCOM Inter-Agency Legal Conference (18 September 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm [last accessed: 16 December 2013 at 07:42].

Reports

1. Final report to the prosecutor by the committee established to review the NATO bombing campaign against the Federal Republic of Yugoslavia, http://www.icty.org/x/file/About/OTP/otp_report_nato_bombing_en.pdf [last accessed: 17 December 2013 at 12:12].

Resolutions

1. Security Council Resolution 713 25 September 1991.
2. Security Council resolution 1031 15 December 1995.