INTERNATIONAL LEGAL ASPECTS OF INFORMATION OPERATIONS

Karl F. Muusse
Staff of the Commander-in-Chief
Directorate of Materiel, Procurement Support Branch
Royal Netherlands Air Force

ABSTRACT

This article explores the international legal rights for states to conduct Information Operations during peacetime and discusses the appropriateness of applying the law of armed conflict to Information Operations during armed conflicts. International law does not explicitly prohibit Information Operations as such, therefore the general principles of international law have to be studied, although Information Operations challenges some fundamentals of international law like the territorial sovereignty of states.
International law contains two important exemptions to the ban. The first is the use of force with the explicit authorisation of the Security Council. To be able to authorise the use of force, the Security Council has to determine whether a threat to the peace etc. has occurred. The second exemption is the use of force in self-defence. When an information attack is launched upon a nation, there is no doubt that this nation has the right to react if the attack can be assessed as an armed attack. Actions taken in self-defence presume a degree of certainty of the identity of the attacker and of the intent of the attacker which in Information Operations often will be a problem.
Information Operations can, by way of disturbing information technology infrastructure which are protected by several international agreements, also constitute forbidden interventions 'below the threshold of the use of armed force'. When the actual hostilities commence, the law of armed conflict becomes valid. This law contains several basic principles codified in many conventions. The conventions apply whenever there is an 'armed conflict'.
The conduct of Information Operations on both sides can constitute an armed conflict, so the principles of the law of armed conflict like 'military necessity', 'humanity', 'distinction' and 'proportionality' do apply

INTRODUCTION

"At the end of 1998 a hacker group, 'Legion of the Underground', declared the 'cyberwar' to China and Iran, and just a few days later also Mexico was virtually offended by a guerrilla group acting under the name 'Intercontinental Cyberspace Liberation Army'. Cyberwar can hurt: according to American Defence specialists, the Russians would possess virus 666, which should be able to bring users of computers in trance and to cause severe spasms of the heart. The East Timor independence fighters acquired an international 'country code' and related to that an official domain name (like .nl for The Netherlands). In January 1999, the East Timor domain, as provided by an Internet service provider in Ireland, and the East Timor website content was attacked by hackers (in this case referred to as E-nazi's). The E-nazi's would have been acting under authority of Indonesia. The 'defence line' of the Irish provider Connect-Ireland broke down after eighteen simultaneous attacks by robots from different

countries", so far a recent statement from the 'Volkskrant'[1].

The rise of the information society confronts governments with important problems on several different subjects, problems that sometimes are strongly linked together. Beside problems as how to optimally facilitate the electronic social intercourse and how to guarantee elementary provisions necessary for the social functioning of citizens and companies in the electronic society, governments are also faced with the fundamental problem how to warrant core values of a democracy in the information society. These values can be at stake by gross violation of privacy rights, by criminal acts as distribution of child porn on the Net, or by threats to the internal and external security of a state. Security threats have changed and perhaps have significantly increased through the worldwide explosion of information technology. The development of the Internet has resulted in a global society dependent on IT[2]. The technological changes that have taken place, termed as 'the Revolution in Military Affairs' or 'the Third Wave' [3], faces governments with new threats and requires reviews of notions of how security threats should be dealt with. In short, these threats and the way they threats are countered can be characterised as 'information operations'. Other writers use terms as 'Netwar', 'Command and Control Counterwar', 'Third-Wave war', 'Knowledge war', and 'Cyberwar'[4].

In this article 'information operations' will be defined according to the NATO definition: *"Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, C2 systems, and CIS while exploiting and protecting one's own information and/or Information Systems"*[5]. Although this NATO-definition creates some confusion using the phrase *"exploiting one's own Information System"*, physical attacks on information systems by traditional military means as well as psychological operations, military deception, and 'electronic warfare' operations, such as jamming radar and radio signals are supposed to be included in this definition.
It is clear that information operations in this definition contains a defensive and an offensive part, it may also be obvious that in practice there is no clear drawing line between defensive and offensive Information Operations. For instance, defensive Information Operations include the capability to assess the ability of an adversary to conduct offensive Information Operations. This assessment can in many times only be made with an intrusion in the information system of the adversary. How then is this assessment to be characterised? Defensive or offensive? Although the scope of Information Operations in this definition is rather broad, this article, when considering what means are used, will primarily deal with the concept of Information Operations as the use of Information Technology. In this article the term 'Information Attack' will be used to describe the offensive part of of Information Operations.

The focus of this article is to search for the international legal implications of Information Operations. The international legal questions concerning Information Operations sound traditional. Does Information Operations constitute aggression, is it a use of force against the territorial integrity, is it an armed attack against which states have the right of self-defence, is that right of self-defence limited to using the same information means, does it constitute a non-armed intervention, what legal rights does a state have if so? What are the implications of the law of armed conflicts on Information Operations?
To answer these questions, this article first explores the international legal rights for states to conduct Information Operations during peacetime. The article then discusses the

appropriateness of applying the law of armed conflict to Information Operations during armed conflicts. This article does not discuss national legal aspects of Information Operations, although there are several important aspects concerning topics like privacy rights of citizens and employees.

INTERNATIONAL LAW AND THE USE OF FORCE IN PEACETIME

International law.

International law consists of binding legal obligations among sovereign states and some of the international organisations. Sovereign states generally assume legal obligations only by affirmatively agreeing to do so. The most effective instruments in creating international law are international agreements. Beside these agreements there is also a body of customary international law, which consists of practices that have been so widely followed by the community of nations, with the understanding that compliance is mandatory, that they are considered to be legally obligatory.
Perhaps because of the newness of much of the technology involved, there is no international agreement that explicitly prohibits Information Operations. The absence of explicit prohibitions is significant because, as a crudely general rule, that which international law does not prohibit it permits. But the absence is not dis-positive, because even where international law does not purport to address particular weapons or technologies, its general principles may apply to their use. When applying these general and longstanding international legal principles however, some basic problems or challenges arise.

Legal challenges.

Two important challenges are to be mentioned[6]: Firstly, simply stated, international law defines war and peace. In making this distinction the 'level' of damage done is a criterion. The sort of damage that information attacks may cause may be analytically different from the physical damage caused by traditional warfare. The kind of destruction that bombs and bullets cause is easy to see and understand, and fits well within long-standing views of what war means. In contrast, the disruption of information systems, including the corruption or manipulation of stored or transmitted data, may cause intangible damage, such as disruption of civil society or government services that may be more closely equivalent to activities such as economic sanctions that may be undertaken in times of peace. This means that Information Operations further blur the already so often unclear line between war and peace.

Secondly, the subjects of international law are foremost states. States are entities, which have sovereign authority over a certain territory. The ability of signals to travel across international networks or through the atmosphere as radio waves challenges the concept of national, territorial sovereignty. Sovereignty holds that each nation has exclusive authority over events within its borders. Sovereignty may be at odds with an increasingly networked, or 'wired' world, as signals travel across networks or as electromagnetic waves, crossing international borders, quickly and with impunity, allowing individuals or groups to affect systems across the globe, while national legal authority generally stops at those same borders. Furthermore, the intangible violation of borders that signals may cause may not be the sort of violation

traditionally understood to be part of a military attack.

Bearing these challenges in mind, I will now discuss the general principles of international law concerning the use of force and apply them to Info Ops. In this discussion the difference between the concepts of 'armed force' and 'force' will be explored. In the subsequent part I will pay attention to the legal principles concerning acts that are 'short of force' or that do 'not amount to the use of force' and relate them to Information Operations.

BAN TO THE USE OF FORCE.

Since the end of the Second World War, the legal rights of states to resort to force in their international relations, traditionally referred to as '*ius ad bellum',* have been first of all laid down in the UN Charter. One of the primary goals of the UN, presently consisting of 188 nations, is to 'unite our strength to maintain international peace and security, and to ensure by the acceptance of principles and institution of methods, that armed force shall not be used, save in the common interest'[7]. It should be noted that the UN Charter does not know the concept of 'acts of war'. So, the often seen title of articles concerning legal aspects of Information Operations *"Is a cyber attack an act of war?"* are not legally relevant.

Armed force.

The question *"Is a cyber attack a 'use of armed force' "* is more relevant since article 2(4), often viewed as the cornerstone of the Charter, prohibits 'the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purpose of the UN'. The prohibition of article 2 (4) is part of '*ius cogens'*, i.e., it is accepted and recognised by the international community of states as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same peremptory character[8].

Is an information attack then ' the use of force'? What is 'force'? Force in the sense of article 2(4) is commonly understood as to at least include 'armed force'. The relevant question then is, is an information attack 'the use of arms'? This question can lead to an endless discussion. With Jacobson I would state that 'armed' simply means equipped with the weapons of war. Armed does not necessarily need to refer only to weapons that cause physical destruction [9]. The use of non-lethal weapons, such as sticky foam, certainly is understood as the use of arms. The conclusion in this opinion is that Information Operations can be the use of armed force and therefore, when it amounts to a level that the territorial integrity or political independence is at stake, be a violation of article 2(4). Criteria to assess whether this level is surpassed are the severity and impact of the damage caused by an information attack and the intent of the attacker. These additional criteria however are not decisive for the assessment whether article 2(4) is violated. Economic coercion measures like an oil boycott for instance, can wilfully cause severe damage, it is commonly not understood however as 'force' in the sense of article 2(4).

Interference short of armed force.

Next to the understanding as force being at least 'armed force' there are also further going

concepts of 'force'. Article 2(4) is elaborated in the General Assembly resolution of 1970 titled as the 'Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations', which is seen as an authoritative restatement of customary international law[10]. This resolution espoused the principle of non-intervention in the *"internal or external affairs of any other state, including armed intervention and all other forms of interference or attempted threats"*. According to some writers it is not possible to conclude anything else then that any interference in the affairs of another state constitutes a violation of article 2(4)[11]. In this perception of the scope of the prohibition of article 2(4) Information Operations can constitute a breach to it, no matter the outcome of the discussion whether Information Operations must be seen as the use of arms.

Exemptions To The Ban On The Use Of Force.

The Charter contains two important and well-known exemptions to the ban on the use of force. The first is the use of force with the explicit authorisation of the Security Council; the second is the use of force in self-defence.

SECURITY COUNCIL RESOLUTIONS

Chapter VII of the Charter constitutes the basis for the Security Council to mandate or, more recently, to authorise the legal use of force by states, acting individually, in ad hoc coalitions or through regional organisations. To be able to mandate or to authorise the use of force, the Security Council, according to the opening article 39, has to determine whether '*a threat to the peace, breach of the peace, or act of aggression'* has occurred.

Threat to the peace, breach of the peace, act of aggression.

The question here is whether an information attack can be a 'threat to the peace, breach of the peace or an act of aggression'? To start with 'acts of aggression' reference can be made to the *"Definition of Aggression"* Resolution of 1974, in which the General Assembly provided what acts by states are seen as 'acts of aggression'[12]. It is obvious that the drafters of this legally not binding resolution were only referring to the arms envisioned at that moment. However, information weapons can easily be seen as part of, for instance, the phrase *"use of any weapon against the territory of another State"*. [13]. With an information attack the 'sovereignty, territorial integrity or political independence' can be at stake, so it can constitute an 'act of aggression' leading to Security Council actions.

In actual UN practice it seems to be more common to conclude that 'threats to the peace' has occurred than to speak of 'acts of aggression'. See for instance Security Council resolution 1199 concerning the Former Republic of Yugoslavia and Kosovo and resolution 1264 concerning Indonesia and East-Timor. In both situations the Council had to balance between the concern of human rights violations and respect for the sovereignty and territorial integrity. Questions that create difficulties for some of the permanent members of the Council, therefore take a lot of time to unanimously address and solve. Is it wishful thinking to assume that information attacks will constitute threats equable important and valid for all of the permanent members? And will it be less politically sensitive? Will the situation be such that Security

Council resolutions, mandating the use of force to counter Info Ops threats, more easily reached than resolutions concerning human rights situations?

Any way, there is no explicit requirement that a 'threat to peace' takes the form of an armed attack, a use of force, or any other condition specified in the Charter. The Security Council has the plenary authority to conclude that virtually any kind of conduct or situation constitutes a 'threat to the peace' in response to which it can authorise remedial action of a coercive nature. Nothing would prevent the Security Council from finding that a Cyber attack is a 'threat to the peace' if it determines that the situation warrants such action. It seems unlikely that the Security Council will take action based on an isolated case of state-sponsored computer intrusion producing little or no damage, but a computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council. The debate in such a case would more likely centre on the offender's intent and the consequences of the offending action than on the mechanism by which the damage was done[14].

All necessary means.

In the case of an information attack that is condemned as 'a threat to the peace' or 'act of aggression', the follow-on question then is how the authorisation to take remedial action of a coercive nature will be or should be formulated? When the Security Council, acting under chapter VII and condemning the information intrusion as an act of aggression or threat to the peace, does not explicitly state that 'all necessary means' can be used, is the use of Information Operations then in line with the mandate? In the UN-vocabulary the phrase 'all necessary means' is used as the most explicit mandate to apply 'armed force' to restore the peace in the specific country or region. When, due to a veto of one of the permanent members of the Council, it would not be possible to get a mandate to use 'all necessary means', it could be doubtful whether Information Operations would then be outlawed.

SELF-DEFENCE.

The second exemption to the ban on the use of force is the use of force in self-defence. Article 51 of the Charter recognises the inherent right of self defence 'if an armed attack occurs'. This article is a source of confusion in the international relations. Is an armed attack different from an 'act of aggression', mentioned in article 39? Does the reference 'if an armed attack occurs' imply that a would-be victim must actually wait for the other side to strike first before it can respond? Does the reference to self-defence as 'an inherent right' indicate that an armed attack may be only one of several circumstances under which action in self-defence could lawfully be undertaken, as it was in the pre-existing customary law before 1945[15]? In 1986 the United States bombed Libya as a response to Libya's continuing support for terrorism against U.S. military forces and other U.S. interests. In June 1993 U.S. forces attacked the Iraqi military intelligence headquarters because the government of Iraq had conspired to assassinate former President Bush. In August 1998 U.S. cruise missiles struck a terrorist training camp in Afghanistan and a chemical plant in Sudan in which chemical weapons should have been manufactured. The rationale articulated for each of these actions was self-defence[16]. The Dutch Government stated that the self-defence claim of the US in the 1998 missile attack was legally right[17]. The Israeli's have long argued and acted according to the doctrine of

‘Nadelstichtaktik’ (needle pricking tactics; ed). This concept holds that although each specific act may not constitute an armed attack, the totality of the incidents might entitle a nation to respond legitimately when the culmination of these acts rises to an intolerable level[18]. This doctrine can be opportune in the case of repeated information attacks, each with only little damage.

The following observations concerning the legality of Information Operations as acts of self-defence can be made:

- When an information attack is launched upon a nation, there is no doubt that this nation has the right to react if the attack can be assessed as an armed attack. The certainty of declarations that Information Operations constitute legitimate acts of self-defence will depend on how the nations and international institutions react to the particular circumstances of the case and of similar cases before. Relevant criteria for this assessment are the damage caused by the attack and the perceived intent of the attacker, more then the means used for the attack. When a power plant is attacked through carbon fire 'bombs' dropped from an aeroplane the consequences could be temporarily as severe as when a physical bomb bombed the plant. In a similar way, when the power plant is neutralised by an information attack the consequences could be equal.

- When a nation chooses to respond to an information attack by mounting a similar computer attack of its own, the issue of whether the initial provocation constituted an armed attack may become a tautology. If the provocation is considered to be an armed attack, the victim may be justified in launching its own armed attack in self-defence. If the provocation is not considered to be an armed attack, a similar response will also presumably not be considered to be an armed attack[19].

- When a nation has proven valid information of a coming attack, it has the right to take action in self-defence. The following conditions might serve as useful guidelines when considering to take action: a clear indication of intent of the adversary; adequate evidence that preparations for the attack have advanced to the point where a attack is imminent; the advantages of the pre-emptive attack must be proportionate to the risks of precipitating a war that might be avoided[20].

- Different reaction scenario’s can be construed. A state can be attacked by an information operation or by an attack with traditional kinetic force. When attacked by electronic means is the state then free to choose the means of reaction or is the state, when it wants to defend itself in a legally correct way, only allowed to react with similar means? The classic requirements when acting in self-defence are of course necessity and proportionality. Proportionality does not necessarily require that an act of self-defence use the same means as the provocation. Conducting a responsive information attack as a measure of self-defence against foreign computer network attacks would have the major advantage that it would minimise the issue of proportionality, which would be more likely to arise if traditional military force were used, such as firing a cruise missile at the building from which a computer network attack is being conducted. Generally speaking, the intensity and scope of self-defence acts should be in line with the attack in order to limit possible escalations of the conflict. In the traditional sense the goal of self defence acts should be to stop the aggressive acts of the adversary and to force him to retreat to his own territory, not to punish or to take revenge. The problem with

information attacks is the fact that it is not possible to force the attacker to retreat, that the exact location of the attacker is unclear and that the intensity of an attack is not always immediately obvious and verifiable. Computer 'time worms' can disrupt information systems months after the intrusion and with in the beginning only little damage. Therefore, a self defence reaction should be allowed also when the only goal can be to dissuade the attacker from a further attack or to degrade him in his ability to undertake a future attack.

Identifying the attacker.

Actions taken in self defence presume a degree of certainty of the identity of the attacker and his intent. In Information Operations this will often be a problem. If the attacker is a State or if the attack is undoubtedly State-sponsored then acts of self defence against that State are legitimate. If the attack is not clearly state-sponsored the question then is in what cases attacks can be at least attributed to a state. Generally speaking, States are not responsible for acts of private persons done on their soil, unless there is a specific protection obligation as for diplomatic personnel. When a nation' s interest is damaged by the private conduct of an individual who acts within the territory of another nation, the normal reaction then will be to notify the government of that nation and to request its co-operation in putting a stop to such conduct. Only if the requested state is unwilling or unable to prevent recurrence does the doctrine of self-defence permit the injured state to act in self-defence inside the territory of another nation[21].

Transit states.

A special topic is the status of nations through whose territory or communications systems a destructive message may be routed. Transit States can be involved in an Information Operation either as a transit medium for the attacker or as a medium for the defender. If only the nation's public communications systems are involved, the transited nation will normally not be aware of the routing a message has taken. If it becomes aware of the transit of an attacker message or a defenders digital bomb, there would be no established principle of international law that it could point to as being violated. Even during an international armed conflict international law does not require a neutral nation to restrict the use of its public communications networks by belligerents. Nations generally consent to the free use of their communications networks on a commercial or reciprocal basis. Accordingly, use of a nation's communications networks as a conduit for an electronic (counter) attack would not be a violation of its sovereignty in the same way as a flight through its airspace by a military aircraft would be.

STATE ACTS 'SHORT OF FORCE'.

International law not only prohibits the use of 'armed force' and other forms of 'force' against other States, it also generally prohibits to interfere in the sovereign rights of that State in order to achieve submission to a foreign will even when the interference has not taken place with the use of force. Only in recent times the notion begins to appear that states loose their right of non-interference by other States in case of gross violations of human rights on their soil. Beside the case of human rights violations, nations whose rights under international law have been violated have the right to take countermeasures against the offending state in

circumstances where neither the provocation nor the response involves the use of (armed) force. Countermeasures can generally be divided in reprisals (measures that are normally violations of treaty obligations or of general principles of international law) and retortions (actions that are unfriendly but do not constitute violations of international law). Information Operations, dependent of several criteria as for instance the severity of the damage done, can constitute interference below the threshold of a 'use of armed force'.

Information systems of the other state can be the object of interference. This can done be against space-based systems, as space segments become more and more critical to many information systems. Several Space law treaties as the Outer Space Treaty of 1967, the Convention on International Liability for Damages caused by Space Objects of 1972 and the Convention on the Registration of Objects Launched in Outer Space of 1975 establish a specific obligation not to interfere with space activities of other nations. Other international agreements to mention here are the 1971 Agreement Relating to the International Telecommunications Satellite Organisation (INTELSAT), the 1976 Convention on the International Maritime Satellite Organisation (INMARSAT) and the European Telecommunications Satellite Organisation (EUTELSAT). These agreements also affect telecommunications and the use of space. The question whether these agreements bar information warfare activities that make use of satellite assets, is dependent on the answer to the question whether these Information Operations are qualified as 'peaceful' or not. Although the agreements in general outlaw use of the satellites for 'military purposes', there are many military applications are granted to the use of these satellites..

Reference can also be made to interference that involves networks and telecommunications. This interference can be a violation of obligations set out in international communications law, most significantly laid down in the International Telecommunications Convention of 1982. Provisions in this Convention seem to block the disruption or spoofing of adversaries' telecommunications. In times of armed conflict these provisions do not apply however.

INFORMATION OPERATIONS AND THE LAW OF ARMED CONFLICT

Whether acting in self-defence or with authorisation of the Security Council or acting as the aggressor, when the actual hostilities commence, the law of armed conflict becomes valid. The law of armed conflict contains several basic principles that are codified in many conventions. Before I will address these principles, two fundamental prerequisites have to be discussed when applying the rules during armed conflicts to information operations.
The first is the so-to-call moment of application of the law of armed conflict; the second is the place of application.

When does the Law of Armed Conflict apply?.

The law of (international) armed conflict applies whenever two or more nation-states are involved in an armed conflict. But what is an 'armed conflict'? The expression 'international (or non-international) armed conflict' is not defined in the Geneva Conventions. Does it require that armed forces engage other armed forces? Must the emphasis lie on physical confrontations and a physical entry of the territory of a foreign state or can virtual

engagements also lead to the application of these traditional rules during armed conflict?
If an information attack does not fit the definition of an 'armed conflict', then many if not all of the laws of armed conflict are not even applicable[22]. With reference to what is stated above concerning the application of the ban on the use of force to Information Operations, the conduct of Information Operations can constitute an armed conflict, dependent again on severity of the damage done, intent of the attacker and the type of countermeasures of the attacked state.

Where does the Law of Armed Conflict apply?..

The law of armed conflict deals with the issues of laws of war on land or at sea. Even the 1977 protocols to update the Geneva Conventions of 1949 continued this connection to the land or sea, while other law of war treaties dealt with the air and space. This corporeal division worked well for first- and second-wave societies dealing with agrarian and industrial matters, but falls short in proscribing conduct in the information age characterised as the third wave society. Information warfare takes place in what has come to be known as cyberspace, an ethereal place that does not neatly fit into the land, sea, air, and space dichotomy[23].

GENERAL PRINCIPLES.

The four fundamental principles of the law of armed conflict are military necessity, humanity, distinction and proportionality. I will briefly discuss these principles and apply them to Information Operations.

Military necessity.

Military Necessity permits that degree of regulated force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with the least expenditure of life, time and physical resources. Many information warfare weapons may not be considered 'regulated force'. This is especially true if they are not set to trigger upon the occurrence of a certain event, but are triggered randomly.
The stipulation that the submission of the enemy be accomplished with the least expenditure of life, time, and physical resources favours Information Operations. Information warfare is largely viewed as a bloodless type of warfare; it can take little time, as it can potentially travel at the speed of light.

Humanity.

The principle of Humanity prohibits the employment of any kind or degree of force not necessary for the purposes of war. The law of land warfare forbade the employment of '*arms, projectiles, or material calculated to cause unnecessary suffering'*. The 1981 Weapons Convention[24] identified, in until now four protocols, weapons that are deemed to be excessively injurious or that are deemed to have indiscriminate effects. Among the weapons banned in these laws are 'dum-dum bullets, projectiles filled with glass or other non-detectable fragments and laser weapons specifically designed to cause permanent blindness. The law of armed conflict requires any nation desiring to implement a new type of weapon to make a determination, prior to its use, regarding its compliance with the principle of

humanity[25]. Terming computer programs as 'weapons' may trigger the required review. At first view it seems safe to state that information 'weapons' more comply with the principle of humanity than most other weapon do.

Distinction.

A central principle is the principle of distinction. Attacks are to be directed at military targets and not at civilian objects, only at combatants and not at civilians. The law of armed conflicts currently defines combatants as 'any member of the armed forces of a party to the conflict'[26]. As only combatants are permitted to take a direct part in hostilities it follows that they may be attacked. Concerning Information Operations some difficult issues may arise: the nature of information systems makes them accessible to a wide group of people, not just enemy soldiers. The teenage hacker of an enemy country who decides to support his country by breaking into the computers of the other state, is he a combatant? The Kosovo-crisis showed that these questions are not hypothetical. Additional Protocol I makes it clear that this hacker can only be a combatant when he is a member of the armed forces or other organised groups that are a party to the conflict, when he serves under effective discipline and when he will be under command of officers responsible for their conduct. If he is not, and it seems to me that this is mostly the case, he is not entitled to the combatant-status. As a civilian he enjoys overall protection to the dangers of military operations [27]. This protection however seizes to exist when the hacker takes a direct part in the hostilities [28]. If combatants acts are conducted by unauthorised persons, like the teenage-hacker, their government may be in violation of the law of armed conflict, depending on the circumstances, and the individuals concerned are at least theoretically subject to criminal prosecution either by the enemy or by an international war crimes tribunal. The long-distance and anonymous nature of computer network attacks may make detection and prosecution however unlikely[29].

The law of armed conflicts also requires making a distinction between military targets and civilian objects. Military targets are defined as '*those objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definitive military advantage*'[30]. In practice for the target-selectors this definition does not make it always clear which target is permissible. During the Kosovo-crisis for instance NATO attacked on 23 April 1999 the Yugoslavian Serb broadcast station in Belgrade. Discussions still continue whether this was a permissible military target.
The dual-use nature of many telecommunications networks and much equipment contribute to the blurring of the distinction between military and civilian systems and, consequently, between military targets, which are legitimate and civilian ones, which are not. Some information weapons may not permit their users to distinguish between military and civilian targets. In the United States, for example, it has been estimated that 95% of the telecommunications of the Department of Defense travel through the Public Switched Network, and during the Persian Gulf War, commercial communications satellites reportedly carried almost a quarter of the U.S. Central Command's transcontinental telecommunications. The interdependence and interconnectivity of civilian and military systems may further exacerbate the difficulty in distinguishing among civilian and military targets. Attacks directed at predominantly military targets may cause civilian systems that are connected to those military systems to fail; alternatively, a virus that is directed toward an adversaries military systems may spread, inadvertently or otherwise, into civilian (and even friendly)

systems [31].

Proportionality.

The principle of distinction is closely related to the principle of proportionality. This principle requires armed forces to use force no greater than necessary to accomplish legitimate military objectives. It also seeks to prevent forces from attacking in situations where civilian casualties would clearly outweigh military gains. The rule is more easily stated than applied in practice, especially in the case where in adopting a method of attack that would reduce incidental damage the risk to the attacking troops is increased[32], as may have been the case in the Kosovo-crisis.
The weapons of information warfare must severely impact an entire network of information systems and all the users of those systems, military and civilian. Denying all information-transfer media and disrupting or destroying every transmission goes beyond a military objective by incapacitating the entire civilian populace as well. Taking out all information-transfer media could bring down a country's stock market, banking system, air traffic control, emergency dispatches and more, leading to civilian casualties and a disproportionate effect as compared to the military objective.

CONCLUSION

The information society creates important problems. Governments are faced with the fundamental problem how to warrant core values of a democracy in the information society. These values can be at stake by threats to the internal and external security of a state. Information Operations can be applied both during peacetime and during armed conflicts. Article 2(4) of the Charter of the UN bans the use of force between states.At this pointthe conclusion has to be that there are different opinions in International Law what actions are to be included in the term 'force', only 'armed force' or also other forms of force. This complicated matter is far from being solved.

---

1 Volkskrant (Dutch daily newspaper), 4-9-1999.

2 Elliot Cohen, A Revolution in Warfare', Foreign Affairs 75/2, April 1996

3 A. And H. Toffler, The Third Wave, Bantam Books 1984, New York

4 R.W. Aldrich, The international legal implications of information warfare, INSS Occasional Paper, April 1996

5 NATO MC 422

6 Greenberg/Goodman/Hoo, Information Warfare and International Law, National Defense University Press

7 Preamble of The UN Charter

8 B. Simma, 'NATO, the UN and the Use of Force: Legal Aspects, European Journal of International Law, Volume 10, nr.1, 1999

9 M.R. Jacobson, War in the Information Age: International Law, Self-Defence, and the Problem of "Non-Armed-Attacks", in: Journal of Strategic Studies, Vol.21, No.3 (September 1998), p.15.

10 UN GA res. 2625

11 For instance, O. Schachter, International Law in Theory and Practice 1991, p. 111.

12 UN GA res. 3314. Article 1. Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.
Article 2. The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.
Article 3. Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of Article 2, qualify as an act of aggression:
(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
(b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
(c) The blockade of the ports or coasts of a State by the armed forces of another State;
(d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

13 Ibid, article 3(b).

14 Department of Defense, Office of General Counsel, An assessment of International Legal Issues in Information Operations, May 1999

15 A. Arend & R. Beck, International Law and the use of Force, Routledge 1993, p.36

16 Department of Defense, Office of General Counsel (note 14), p.12.

17 Letter of the Secretary of State to the Parliament, 10 February 1999

18 H. McCoubrey/N. White, International Law and Armed Conflict, England 1992, p. 36.

19 Department of Defense, Office of General Counsel (note 14), p.18.

20 M.R. Jacobson (note 9), p.15.

21 Department of Defense, Office of General Counsel (note 14), p.23.

22 See Aldrich (note 4), p. 4.

23 Ibid note 22

24 Formal title: United Nations Convention on Prohibitions or Restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects.

25 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 36.

26 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 43.

27 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 51, para 1.

28 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 51, para 3.

29 Ibid, note 6

30 Additional Protocol I (1977) to the Geneva Conventions of 1949, article 52, para 2.

31 Ibid, note 6

32 A.P.V. Rogers, Law on the battlefield, Manchester/New York 1996, p.17