EUI Working Papers

AEL 2010/2
ACADEMY OF EUROPEAN LAW
PRIV-WAR project

Legal Implications of the Privatization of Cyber Warfare

Lucas Lixinski

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE

ACADEMY OF EUROPEAN LAW

Legal Implications of the Privatization of Cyber Warfare

LUCAS LIXINSKI

EUI Working Paper **AEL** 2010/2

The 'Regulating Privatisation of "War": The Role of the EU in Assuring the Compliance with International Humanitarian Law and Human Rights" (PRIV-WAR) project is funded by the European Community's 7th Framework Programme under grant agreement no. 217405.

This paper was produced as part of the EUI contribution to the PRIV-WAR Project.

www.priv-war.eu

ISSN 1831-4066

Printed in Italy
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Abstract

The paper deals with the combination of two emerging topics in militarization and the conduct of war: cyber warfare and the use of private military and security companies and personnel. As technological capacity grows, populations and governments alike become more and more dependent on reliable internet connections and information placed only on the cyberspace. The fact that computers are so depended upon makes these sectors of human activity particularly vulnerable if their computers or networks were to be shut down. One equally important topic is that of the privatization of war. This is an increasingly strong tendency among governments, who look at privatization as the answer to their needs for not having to maintain a large permanent military and seek more efficiency in methods and operation. But what happens when cyber warfare is privatized, when a contractor working simultaneously for the U.S., French and Saudi Arabian governments can, from his office in a commercial neighbourhood in London, set off an attack that disrupts the entire telecommunications grid of say, China? The topic of the privatization of cyber warfare seems to float in a “double legal vacuum”, as there are no clear rules for either cyber warfare in general or for the privatization of military services. However, I suggest that rules can be drawn analogically from established rules and principles of international humanitarian law and human rights to fill both of these vacuums.

Legal Implications of the Privatization of Cyber Warfare

LUCAS LIXINSKI[*]

1. Introduction

One of the most important emerging topics related to militarization and the conduct of war is that of cyber warfare.[1] As technological capacity grows, populations and governments alike become more and more dependent on reliable internet connections and information placed only on the cyberspace. The whole financial market can no longer function without the internet and computers generally. The same can be said of air traffic and other sectors that would at first sight seem less network-dependant, such as energy distribution systems and hospitals. The fact that computers are so depended upon makes these sectors of human activity particularly vulnerable if their computers or networks were to be shut down.

One equally important and emerging topic is that of the privatization of war, or the reliance upon contractors, Private Military and Security Companies (PMSCs) and other similar actors for the performance of duties that once fell under the exclusive domain of the State and its armed forces. This is an increasingly strong tendency among governments, that look at privatization as the answer to their needs for not having to maintain a large permanent military and seek more efficiency in methods and operation. This is what has been known as "the Rumsfeld Doctrine" with regard to the U.S. military,[2] but it is also the case in many other countries.

Companies such as Xe Services LLC (formerly known as Blackwater International) and Executive Outcomes are known for being able to tip the balance in several conflict zones and bring a quick end to hostilities, regardless of what one may think about them.[3] They can help stop a *coup d'état* in Angola, and provide effective security for high-level diplomats in Iraq, for instance.

In May 2009, the U.S. Presidency published a report called "Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communication Infrastructure". In this report, the White House recognized that the U.S. had lagged behind in its response to the growing threat of cyber attacks, and it went on to highlight the importance of cooperation with the private sector.[4] This has spurred a surge

---

[*] Ph.D. Researcher, European University Institute (Italy); LL.M. in Human Rights, Central European University (Hungary); LL.B., Federal University of Rio Grande do Sul (Brazil). MAE-AECI Fellow (Spain). This paper has been written within the broader context of a collaborative research project funded by the European Union, called PRIV-WAR – Regulating Privatization of War. I am thankful to Professor Francesco Francioni for the invitation to take part in this project and the feedback on an earlier draft, to Oleksiy Kononov for his help in translating a Russian text used in this article, and to an audience in Rio de Janeiro for their input. All errors remain my own. E-mail: Lucas.Lixinski@eui.eu.

[1] Also known as internet warfare, cyber war, and information warfare, among other synonyms. For the purposes of this paper, these terms will be used interchangeably, unless otherwise indicated.

[2] For an explanation of the Rumsfeld Doctrine, as well as excerpts from a speech given by Donald Rumsfeld on September 10, 2001, regarding the need for an entrepreneurial approach to the military, *see* JEREMY SCAHILL, BLACKWATER – THE RISE OF THE WORLD'S MOST POWERFUL MERCENARY ARMY 49-51 (2008).

[3] On Blackwater International, *see* JEREMY SCAHILL, BLACKWATER – THE RISE OF THE WORLD'S MOST POWERFUL MERCENARY ARMY (2008). On Executive Outcomes' activity in Angola, *see* P.W. SINGER, CORPORATE WARRIORS – THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 107-110 (2008).

[4] *See* STUART S. MALAWER, CYBERWARFARE: LAW AND POLICY PROPOSALS FOR U.S. AND GLOBAL GOVERNANCE, *available at* <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1437002> (last accessed September 25, 2009).

among military contractors and IT companies who started recruiting personnel and preparing themselves for the opening of tender processes before the U.S. military.[5]

It has been reported that all major U.S. military contractors have contracts in the field of cyber warfare with the military and intelligence agencies. These companies, further, have been cooperating towards building a "Cyber Range", or a duplicate of the internet where they can test offensive and defensive techniques for cyber warfare.[6]

Along these lines, the United States Special Operations Command (USSOCOM) has, in its strategic plan for 2009, outlined the need for investment in cyber warfare capacity. However, unlike the White House report, this one focuses on the development of in-house capacity for cyber warfare, and, more specifically, network-centric capabilities.[7]

What happens, however, when both of these emerging phenomena cross paths? Namely, what happens when cyber warfare is privatized, when a contractor working simultaneously for the U.S., French and Saudi Arabian governments can, from his office in a commercial neighborhood in London, set off an attack that disrupts the entire telecommunications grid of say, China? Who is responsible for the attack? And, more importantly, what happens when, by disrupting the telecommunications system, one satellite happens to fall back into the atmosphere, crashing into a school in South Korea, killing dozens of innocent children? Who bears responsibility for these issues? Is it the British government, for letting this person use its cyberspace to launch the attack? Is it one or all of the government of the States under whose service this contractor acts? Is it the Chinese government, to whom the satellite belonged?

These are some of the questions this article explores. This article deals with the topic of the privatization of cyber warfare and the legal consequences of violations of international humanitarian law (IHL) and human rights perpetrated in cyber conflict scenarios.

The topic of the privatization of cyber warfare seems to float in a "double legal vacuum", as there are no clear rules for either cyber warfare in general or for the privatization of military services. However, I suggest that rules can be drawn analogically from established rules and principles of IHL and human rights to fill both of these vacuums.

The paper will be structured as follows: the first part will look generally at cyber warfare, exploring the modalities in which it occurs, and the possibilities for regulation of it, both in international humanitarian law and general human rights law. My contention is that cyber attacks differ substantially from each other, and that not all cyber attacks meet the necessary threshold for calling international humanitarian law into application. There are, however, several rules that should be observed even when the gravity of a cyber attack does not amount to an "act of war".

The second part is a reflection on the privatization of cyber warfare. It starts by examining recent policy developments that discuss the structuring of cyber warfare, as well as the argument of the supposed inextricability of the private sector from this area of the military. It then analyzes the issue of accountability of "private cyber warriors" for acts that violate human rights and humanitarian law.

---

[5] *See* Christopher Drew and John Markoff, *Contractors Vie for Plum Work, Hacking for U.S.*, NEW YORK TIMES (MAY 30, 2009), *available at* <http://www.nytimes.com/2009/05/31/us/31cyber.html> (last accessed September 25, 2009).

[6] *See* Christopher Drew and John Markoff, *Contractors Vie for Plum Work, Hacking for U.S.*, NEW YORK TIMES (MAY 30, 2009), *available at* <http://www.nytimes.com/2009/05/31/us/31cyber.html> (last accessed September 25, 2009).

[7] *See* UNITED STATES SPECIAL OPERATIONS COMMAND, USSOCOM CIO STRATEGIC PLAN 2009, *available at* <http://www.socom.mil/SOCOMHome/newspub/pubs/Documents/CIO_Strategic_Plan-2009.pdf> (last accessed September 25, 2009).

2. Cyber Warfare

The aim of this part is to refute the idea of the "legal vacuum" of cyber warfare under currently existing international law, and idea that many have been quick to affirm.[8] While it is true that more specific rules are necessary to address the specificities of cyber warfare, it is an exaggeration to say that there are no applicable rules at the moment that can help deal with certain situations should they arise before a specific instrument is completed.

However, before debating this issue, it is important to understand what falls under the category "cyber attack", and the effects of different types of technology-based warfare. To this effort I move first.

A. Fighting a Cyber War

Cyber war falls under the broader definition of "information warfare". Information warfare, according to military sources, falls into three categories: (1) acts aimed at "maintaining information superiority while protecting against counter-information warfare"; (2) "using information as a weapon against the enemy", or (3) the use of information systems to enhance the effectiveness of the use of force.[9]

The first two categories refer more broadly to intelligence and information gathering, whereas the third one refers to "technology-based warfare" in a strict sense. There are two main types of action that can be described as "technology-based warfare", and that rely heavily on the cyberspace. The first one is what is known as "network-centric combat". In this type of combat, soldiers are normally deployed to the field. The big difference is that they rely heavily on intelligence information and technology that enhances their capabilities, such as Global Positioning System packages, constant communication links with information units off the theater of war who keep feeding the soldiers with useful intelligence, equipment that can pick up on radio transmissions and from that determine the position and movement of enemy combatants, among others.[10]

While this is an important use of technology and the internet to enhance combat capabilities, this is not cyber warfare in the strict sense. However, there are specific implications to be taken into account here. For instance, the definition of combatant defines a combatant as a person engaging directly in hostilities.[11] Until recently, this meant only the soldiers in the theater of conflict, as any information was given to them prior to actual combat, and therefore intelligence agents did not participate in hostilities. However, direct and constant communication links imply that people far from the actual theater of conflict, sometimes sitting in offices thousands of kilometers away, in a civilian zone in a different country, are also participating moment by moment in hostilities. Are these people also to be

---

[8] *See* for instance U.S. JOINT CHIEFS OF STAFF, QUESTIONS ABOUND IN CYBER THEATER OF OPERATIONS, VICE CHAIRMAN SAYS, *available at* <http://www.jcs.mil/newsarticle.aspx?ID=106> (last accessed September 23, 2009).

[9] As cited by Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. ILJ 179, 184 (2006).

[10] For an explanation of network-centric warfare, *see* Stuart H. Starr, *Toward a Preliminary Theory of Cyberpower*, *in* CYBERPOWER AND NATIONAL SECURITY 43, 59-60 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009). On the dependence of network-centric warfare on intelligence gathering, *see* TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING 162-163 (2009). Martin C. Libicki questions whether network capabilities actually enhance combat performance, and concludes that there is no measurable impact on combat effectiveness. *See* Martin C. Libicki, *Military Cyberpower*, *in* CYBERPOWER AND NATIONAL SECURITY 275, 284 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

[11] For a list of definitions of "combatant" extracted from military handbooks, *see* Thomas C. Wingfield, *International Law and Information Operations*, *in* CYBERPOWER AND NATIONAL SECURITY 525, 534 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

considered combatants? While they cannot physically engage with enemies, they are an indispensable part of the capabilities of the soldiers on the field to engage enemies, and can make a significant difference in the outcome of a war, as they serve practically as the "super eyes" of soldiers. Another example of this kind of activity is the use of remote control-operated drones that can bomb a target without the need for someone to be physically present to launch or detonate it.[12]

I submit that they should be considered combatants. And this implies that the communication links they use, as well as their equipment, are legitimate military targets, either through cyber attacks or physical strikes (for instance, bombing the building where the computers used for information gathering and transmission are). But this also implies that the equipment cannot be placed amidst civilian property or otherwise protected property, as defined by international humanitarian law rules.

But the most important type of technology-enabled warfare for our purposes is what is known as cyber attacks. Any attempt at defining a cyber attack would necessarily be broad and rather vague, but a working definition would be attacks conducted with the primary use of the internet with the goal of inflicting temporary or permanent harm to information systems, with or without consequences to the physical support of these systems or any other physical objects connected to them.

Some of the tactics used in cyber warfare include: espionage and intelligence gathering; "web vandalism", or attacks aimed at defacing web pages, or causing servers to collapse by flooding it with innumerable requests through what is known as "Denial of Service" (DoS) attacks (which is what happened in Estonia in 2007);[13] the posting of propaganda on the internet;[14] distributed DoS attacks, which is a much stronger version of a normal DoS attach, in which a single person controls, through spyware software, worms and other malicious software a large number of computers, which are all used to launch a DoS attack against a larger system; and disruption of equipment, by for instance disrupting the communications system of precision bombs,[15] or paralyzing software that controls the cooling system of a group of satellite antennas.[16]

The disruption of equipment can happen through the launching of viruses into the operational systems of the equipment to be affected, or by launching an Electronic Magnetic Pulse weapon against the targeted structures (that is, the building where the computers that command the equipment is). While this is an effective and seemingly "least destructive" alternative to the bombing of a building, it can

---

[12] Questioning the morality of using drones to promote targeted killings, *see* Roger Cohen, *An Eye for an Eye*, THE NEW YORK TIMES, FEBRUARY 25, 2010, *available at* <http://www.nytimes.com/2010/02/26/opinion/26iht-edcohen.html?th&emc=th> (last accessed February 26, 2010).

[13] *See* Edward Skoudis, *Information Security Issues in Cyberspace*, *in* CYBERPOWER AND NATIONAL SECURITY 171, 177-178 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009); and Thomas C. Wingfield, *International Law and Information Operations*, *in* CYBERPOWER AND NATIONAL SECURITY 525, 531-533 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009)..

[14] *See* MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 30 (2007).

[15] In this specific example, the precision bomb becomes an indiscriminate weapon, and serious collateral damage can be done by it, so the lawfulness of such use of a cyber attack is questionable. *See* William Church, *Information Warfare*, 837 INTERNATIONAL REVIEW OF THE RED CROSS 205 (2000), *also available at* <http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/57jqcz?opendocument> (last accessed September 24, 2009).

[16] This is only a sample list. Many authors have created their own lists, more or less comprehensive than this one. *See* MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 31 (2007) (with a very useful diagram), and again at 79-87; Christopher C. Joyner and Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EJIL 825, 836-839 (2001).

also cause a lot of collateral damage, as the pulse will affect all computers within a certain radius of its deployment, which can affect vital civilian systems.[17]

Other techniques include the use of computer attacks to add imaginary targets to enemy computers (causing the enemy to waste efforts and weapons, and ultimately breaking the enemy's confidence as, once the enemy realizes it has been deceived once, it will hardly be sure again of whether a target is a real or false target).[18]

Cyber attacks can be of two types, according to their consequences: there are cyber attacks the consequences of which are limited to the virtual world (such as attacks on websites and DoS attacks),[19] while others may cause very tangible damage in the physical world (e.g., stopping a country's electrical power distribution system, or causing a nuclear plant to collapse by disrupting its computer-operated cooling system).[20]

Some of the effects that can be obtained through cyber warfare are: (1) the destruction or disruption of infrastructure systems; (2) distracting the military, or diverting its energies, from detecting physical impending attacks[21] (referred to in military circles as "hybrid warfare");[22] (3) intelligence theft;[23] (4) general effects on military and civilian morale, which can be a side effect of an attack on another target, or the primary objective (such as propaganda built into governmental websites, or simply the psychological effect of having some concept of "social integrity" breached from abroad).

---

[17] *See* William Church, *Information Warfare*, 837 INTERNATIONAL REVIEW OF THE RED CROSS 205 (2000), *also available at* <http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/57jqcz?opendocument> (last accessed September 24, 2009).

[18] *See* MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 52 (2007); and William Church, *Information Warfare*, 837 INTERNATIONAL REVIEW OF THE RED CROSS 205 (2000), *also available at* <http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/57jqcz?opendocument> (last accessed September 24, 2009). Martin Libicki, a representative from the private military industry who wrote the book used in this article, tells an interesting anecdote in this sense: "[…] When Winston Churchill during World War I proposed dragging battleship silhouettes in the water, sceptics replied that the Germans would eventually realize that they were being tricked; he responded that henceforth they would doubt their eyes whenever they saw any such silhouette, whether real or fake." *Id*.

[19] *See* David E. Sanger, *U.S. Steps Up Effort on Digital Defenses*, NEW YORK TIMES (APRIL 27, 2009), *available at* <http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=1&adxnnl=1&adxnnlx=1253975270-G+kOz52VSudZlgfg7AUxRA> (last accessed September 23, 2009). This is what he reported on the use of these techniques in the context of the Georgia-Russia conflict of 2008: "In August 2008, when Russia invaded Georgia, the cyberattacks grew more widespread. Georgians were denied online access to news, cash and air tickets. The Georgian government had to move its Internet activity to servers in Ukraine when its own servers locked up, but the attacks did no permanent damage."

[20] *See* GREGORY J. RATTRAY, STRATEGIC WARFARE IN CYBERSPACE 19 (2001).

[21] *See* William Church, *Information Warfare*, 837 INTERNATIONAL REVIEW OF THE RED CROSS 205 (2000), *also available at* <http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/57jqcz?opendocument> (last accessed September 24, 2009) (pointing out for the possibility of engaging in such actions against civilian infrastructure prior to the start of hostilities, as a means to delay physical conflict).

[22] *See* David E. Sanger, *U.S. Steps Up Effort on Digital Defenses*, NEW YORK TIMES (APRIL 27, 2009), *available at* <http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=1&adxnnl=1&adxnnlx=1253975270-G+kOz52VSudZlgfg7AUxRA> (last accessed September 23, 2009).

[23] For instance, it has been reported that in March 2009 a spy network using computers located mainly in China has retrieved classified information from computers of governments and private organizations in 103 countries, including computers of Tibetan exiles. China has denied any participation in these events. *See* MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE'S REPUBLIC OF CHINA, FOREIGN MINISTRY SPOKESPERSON QIN GANG'S REMARKS ON THE SO-CALLED CHINESE CYBER-SPY RING INVADING COMPUTERS IN COUNTRIES, *available at* <http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t555337.htm> (last accessed September 26, 2009); and WIKIPEDIA, CYBERWARFARE, *available at* <http://en.wikipedia.org/wiki/Cyberwarfare> (last accessed September 26, 2009).

All these forms of cyber warfare, as well as their different effects and the different form of classification, indicates that there are very different degrees of intensity of a cyber attack. Consequently, there will also be different legal responses to these different degrees. I will now analyze these different possible legal responses.

B. The Matter of the Applicable Law

1. International Humanitarian Law

Cyber warfare can happen both in times of peace and times of war.[24] Whether it happens during wartime or peace time will determine the legal regime applicable. Also, one has to take into account the different legal perceptions of each individual act of cyber warfare, which, even out of context, can be seen as triggering different regimes.

Depending on the way an act of cyber warfare is legally perceived, there will be a different applicable regime. If an act of cyber war is seen as an act of use of force, than general principles of international humanitarian law should apply. If, on the other hand, one does not look at these acts as meeting the legal threshold for characterizing these acts as an "armed attack" initiating an armed conflict, then the applicable regime should be the incipient international law on cybercrime and the general regime of human rights law.

The definition of international conflict as a threshold for the application of IHL has been determined to be any situation in which a State's armed forces breach the sovereignty of another State.[25] In this sense, a cyber attack, if conducted by persons not enlisted in a State's military forces, could not conceptually be an armed attack. However, one commentator has noted that "the reference to armed forces is more logically understood as a form of prescriptive shorthand for activity of a particular nature and intensity."[26] Taking this into account, and in light of the principles and purposes of IHL, one is led to conclude that an armed attack is an assault upon another State with military means to impinge upon territorial integrity and political independence.[27] This can naturally extend to cyber warfare that is aimed at provoking direct destruction of property or loss of life in the physical world, to the extent one of the effects of these actions is precisely to cause internal unrest and weaken the governmental structure. It encompasses therefore actions aimed at, for instance, altering an airport's air traffic control system (which could lead to airplane collisions), but not necessarily acts aimed at defacing a governmental website.

Moreover, if one chooses to apply IHL, one has to consider the questions of territory as a requirement for the determination of IHL regime. How is the international character of a cyber conflict to be determined? Is to be presumed, or should there be some criteria for this determination? The "place"

---

[24] *See* William Church, *Information Warfare*, 837 INTERNATIONAL REVIEW OF THE RED CROSS 205 (2000), *also available at* <http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/57jqcz?opendocument> (last accessed September 24, 2009).

[25] *See* Thomas C. Wingfield, *International Law and Information Operations*, *in* CYBERPOWER AND NATIONAL SECURITY 525, 526-531 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009); and Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 846 INTERNATIONAL REVIEW OF THE RED CROSS 365, 372 (2002).

[26] *See* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 846 INTERNATIONAL REVIEW OF THE RED CROSS 365, 372 (2002).

[27] Another definition characterizes an armed attack as an act or attempt to destroy, kill or injure, but this definition can be easily mistaken by the use of force by a State's police internally, which surely does not fall within International Humanitarian Law. *See* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 846 INTERNATIONAL REVIEW OF THE RED CROSS 365, 373 (2002).

where the conflict takes place, for instance, cannot be deemed a determining factor, for the computers engaged in the conflict need not be in the territories of the conflicting States.

Also, cyberspace can in itself be referred to as a new environment for military action, and it has been assimilated to the global commons (outer space and the oceans are the most common references) in the literature about it.[28] There are certain differences, of course, at least to the extent that rules governing the oceans do create some sort of jurisdictional allocation, but the rules governing outer space are more easily applicable. And these become very relevant for analogical application: the core international treaty regulating the use of outer space explicitly determines that all activities of non-governmental entities in outer space must be authorized and continuously supervised by States parties to the relevant treaties. States are responsible for activities undertaken in outer space by governmental and non-governmental entities alike.[29] It further determines that States are responsible for damage caused to another State simply if the object that caused the harm has been launched from their territory.[30] Rules governing outer space thus offer interesting insights and can be applied analogically to the regulation of cyber space. One must be aware of differences, however. Possibly one of the reasons why responsibility for the acts of private entities is so easily attributable to the State in the outer space context is that outer space endeavors are large and costly enterprises, and the State from which one such enterprise is launched would hardly be able to deny knowledge of it; when it comes to cyber attacks, however, any person with a home computer can launch one such attack, as long as s/he has the necessary skills and training. This difference of scale and accessibility must be taken into account when trying to draw this parallel, but I suggest that the parallel can be drawn nonetheless.

Another important question is that of attribution. Assuming a cyber attacker does not identify herself / himself, how can this identification be done? Tracing the attack back is a long and often futile exercise, as most cyber traffic goes through a wide range of computers in disparate parts of the world,

---

[28] *See* Franklin D. Kramer, *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, *in* CYBERPOWER AND NATIONAL SECURITY 3, 12 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009); MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 31 (2007); and Stuart H. Starr, *Toward a Preliminary Theory of Cyberpower*, *in* CYBERPOWER AND NATIONAL SECURITY 43, 48 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

[29] *See* TREATY ON PRINCIPLES GOVERNING THE ACTIVITIES OF STATES IN THE EXPLORATION AND USE OF OUTER SPACE, INCLUDING THE MOON AND OTHER CELESTIAL BODIES, Article VI. The full text of the provision is the following: "Article VI**.** States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the Moon and other celestial bodies, *whether such activities are carried on by governmental agencies or by non-governmental entities*, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty. *The activities of non-governmental entities in outer space, including the Moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty*. When activities are carried on in outer space, including the Moon and other celestial bodies, by an international organization, responsibility for compliance with this Treaty shall be borne both by the international organization and by the States Parties to the Treaty participating in such organization." (emphasis added)

[30] Id., Article VII. The full text of the provision is the following: "Article VII. Each State Party to the Treaty that launches or procures the launching of an object into outer space, including the Moon and other celestial bodies, and *each State Party from whose territory or facility an object is launched, is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons* by such object or its component parts on the Earth, in air space or in outer space, including the Moon and other celestial bodies." (emphasis added)

being hardly linear.[31] Also, even if an attack can be traced back to a certain country, it is nearly impossible to determine whether the source is a State- or a privately-owned computer.[32]

Therefore, it would be nearly impossible to attribute an attack through these means. Even if this would be possible, tracking the attack down to its source computer would not necessarily resolve the problem. For one, this computer may be just a smokescreen created by spyware software for the real attacker. Also, as private military contracting expands into cyberwar, to find that the computer responsible for the attack is one of a private military company does not say much, particularly if this company renders services to more than one State. The attacks of March 2009 in which intelligence computers in 103 countries were hacked and had information stolen by computers that could be traced back to China is an example. Even though the attacks were traced back to China, the Chinese government denied any involvement in the acts, and that more or less ended the affair, as there are no means to effectively prove that the attacks were commanded by Chinese authorities.[33]

Further, the fact that there was no response to these attacks may serve as evidence of State practice in not considering them as armed attacks, at least not to the extent that it may trigger the application of Article 51 of the UN Charter (as a use of force) or international humanitarian law. Thus, one may be led to the conclusion that different forms of cyber attack will constitute armed attacks or not depending on the pervasiveness of their effects. Documented cyber attacks have so far done little more than blocking access to or defacing certain websites, and there have been also some alleged thefts of intelligence information. None of this, however, seems to be enough to trigger a military countermeasure, cybernetic or otherwise, which lends further credence to the notion that these forms of cyber warfare at least cannot be deemed to be armed attacks. If a cyber attack, however, ever has effects causing the loss of civilian life and / or property, the response might be stronger. Another possible interpretation is simply that a sufficient causal link between the attacks and the Chinese authorities could not be established. The analogical application of rules on outer space, however, would help shed light onto this situation, as all that would be required would be to determine that the computers were located in China.

If IHL applies, then naturally do the concepts of “protected person” and “protected property”. This means that all attacks directed at non-military cyber structures are to be considered in violation of IHL principles. In this sense, one has to consider that cyber warfare cannot thus be conducted from a civilian building, as this building naturally becomes a legitimate military target due to the presence of the cyber warriors.

Likewise, the computer systems of hospitals and essential public utilities such as power plants can also not be targets of cyber attacks, since they are considered protected property by rules of international

---

[31] *See* Thom Shanker and David E. Sanger, *Privacy May Be a Victim in Cyberdefense Plan*, NEW YORK TIMES (JUNE 12, 2009), *available at* <http://www.nytimes.com/2009/06/13/us/politics/13cyber.html> (last accessed September 25, 2009) (making the case that this may even imply that to counter a cyber attack may require entering the “cyber territory” of third nations).

[32] Recent U.S. efforts to try to determine the source of foreign-originated scans into American industrial databases illustrate this point. It has been reported that, even though it was possible to ascertain that the probing came from China, it was not possible to determine whether it came from the Chinese government or a non-State actor. *See* David E. Sanger, *U.S. Steps Up Effort on Digital Defenses*, NEW YORK TIMES (APRIL 27, 2009), *available at* <http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=1&adxnnl=1&adxnnlx=1253975270-G+kOz52VSudZlgfg7AUxRA> (last accessed September 23, 2009).

[33] *See supra* note 23 and accompanying text.

humanitarian law.[34] Most of the common examples of scenarios of cyber attack are therefore examples of acts that violate general principles of international humanitarian law.

This application of IHL has to do with the concept of collateral damage and the principle of proportionality. Other principles that must be observed include chivalry / the prohibition of perfidy (which requires for instance that cyber attacks be not used to plant false intelligence as a means to mislead adversaries),[35] and the principles of necessity and humanity.[36]

If a cyber attack, however, happens outside of the context of a conflict, and does not amount by itself to an act of use of force, then the rules and principles of international humanitarian law do not apply. Instead, the applicable regime will be that of general human rights law and specific rules on cybercrime.

2. International Human Rights Law

Human rights rules will be applicable as general principles of law, requiring, for instance, that privacy and freedom of expression and information be protected when cyber attacks imply breaking into databases and public and private websites. The situation during the Georgia-Russia conflict,[37] in which access to newspaper websites was denied, is an example of a violation of a human rights rule, as it violated the freedom of expression (seen as the freedom to impart and to receive information) of Georgians..

The early 2010 Google-China controversy is an example of violation of privacy by cyber warfare means, even though ultimately the attacks were directed at a private company, and not at a State. China was allegedly trying to gain information on political activists within its own territory. To this extent, should political opposition in China ever take upon arms, and start an internal conflict in the country, any act such as those against Google and Gmail could be considered an act of cyber warfare in the context of an internal conflict, and in violation of human rights.[38]

---

[34] There are several rules in Additional Protocol I to the Geneva Conventions protecting: installations containing dangerous forces, including most power plants (Article 56); cultural property (Article 53); medical facilities (Article 12); religious buildings (Article 53); farms and crops (Article 54). *See* also Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 846 INTERNATIONAL REVIEW OF THE RED CROSS 365, 385 (2002).

[35] The relevant rule on the prohibition of perfidy is Article 37 of Additional Protocol I. The full text of the provision is the following: "Art 37. Prohibition of Perfidy. 1. It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy. The following acts are examples of perfidy: (a) the feigning of an intent to negotiate under a flag of truce or of a surrender; (b) the feigning of an incapacitation by wounds or sickness; (c) the feigning of civilian, non-combatant status; and (d) the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict.

2. Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation."

[36] For a survey of these principles with regard to cyber warfare, *see* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. ILJ 179, 198-207 (2006).

[37] For more on cyber warfare in the context of this conflict, *see* Daniel T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, *in* CYBERPOWER AND NATIONAL SECURITY 24, 36 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

[38] *See* WIKIPEDIA, GOOGLE CHINA, *available at* <http://en.wikipedia.org/wiki/Google_China> (last accessed February 25, 2010).

If one also considers that other companies have been similarly attacked at the same time, and some of these attacks happened with the purpose of gaining information on weapons systems, the cyber warfare dimension of the incident becomes more immediately palpable. This series of attacks became known as "Operation Aurora" and, at the time of writing, are still ongoing.[39]

Other possibilities for human rights violations arising out of cyber attacks refer to the effects of these attacks upon the physical world. For instance, a cyber attack that leads to the disruption of the power grid of a hospital, causing the loss of patients' lives, can be considered a violation of the right to life. Similarly, a cyber attack that leads to the explosion of a factory and the spilling of toxic content into a river, polluting the water source of a certain city or village, can be seen as a violation of the right to private life, according to a similar precedent of the European Court of Human Rights.[40]

The examples so far are restricted to civil and political rights. Naturally, there are many instances in which economic, social and cultural rights are affected, in part as the counterpart to a civil and political right. In the hospital case, for instance, the right to health is affected; in that of the pollution, the right to a safe environment is being impinged upon. Other examples may include the right to food and water in the case of cyber attacks compromising food distribution schemes, or the right to culture, with the denial of access to information. Be it as it may, acts of cyber warfare have a very tangible impact upon human rights, particularly when the targets of attacks are not military objectives.

When it comes to the enforcement of these rules, however, a serious problem arises in meeting the jurisdictional threshold of most human rights adjudicatory and quasi-adjudicatory bodies, and to connect the case to a State party to a human rights instrument. That is, it is difficult to argue that in the hypothesis of Afghani victims of a cyber attack launched by France in which access to Afghani and foreign media was denied (violating therefore freedom of expression) that the affected Afghani citizens were at any moment under the jurisdiction of France. It has already been established that it is very difficult to establish jurisdiction in the case of aerial bombings,[41] and the same negative of jurisdiction can be transplanted to the context of cyber attacks.

Cybercrime rules, on the other hand, have very limited reach in offering redress to victims of cyber attacks. They offer States tools to prosecute and punish the perpetrators of cyber attacks that fall under the States' jurisdiction, but it does not by itself offer remedies to the victims other than the indirect effects of prosecution and punishment of perpetrators. And this set of rules is only applicable to non-State actors, being unclear whether an attacker acting with State support would be subject to the same rules.

Among the different sets of potentially applicable rules to the general context of cyber warfare, therefore international humanitarian law seems to offer the best structure for dealing with cyber attacks. However, this set of rules is not applicable at all times, and a certain threshold must still be met to trigger the application of IHL principles. Further, the application of IHL rules to private actors engaging in cyber war is difficult. I will now look at the possibilities for holding private actors engaging in cyber war accountable for their actions

---

[39] *See* WIKIPEDIA, OPERATION AURORA, *available at* <http://en.wikipedia.org/wiki/Operation_Aurora> (last accessed February 25, 2010).

[40] See European Court of Human Rights, *Case of López Ostra v. Spain* (Application no. 16798/90), judgment of 9 December 1994.

[41] See in this sense the seminal case of the European Court of Human Rights. ECtHR, *Bankovic* et al *v. Belgium* et al (Application no. 52207/99), Admissibility Decision (Grand Chamber); and Georg Ress, *Problems of Extraterritorial Human Rights Violations – The Jurisdiction of the European Court of Human Rights: the Bankovic Case*, 12 ITALIAN YEARBOOK OF INTERNATIONAL LAW (2002).

3. Privatizing Cyber Warfare: E-Mercenaries?

This part will discuss emerging strategies regarding cyber warfare (offensive and defensive) in a few countries and NATO. It will also discuss whether the involvement of non-State actors in cyber warfare is alike to their involvement in the broader military, or if there is something peculiar to cyber warfare that requires a greater or smaller involvement of the private sector. I will then move on to analyzing issues of accountability and responsibility for actions undertaken by these private individuals in the context of cyber warfare that violated international humanitarian law or human rights rules.

A. Emerging Strategies on Cyber Warfare

The United States has in many aspects taken the lead in the development of cyber warfare. Even though a report issued in April 2009 said that the issue was not addressed properly within the U.S. military, and that there was no real structure for cyber warfare,[42] there have been reports that prior to that the U.S. has engaged in offensive cyber attacks at least twice: once in penetrating Iran's nuclear program for intelligence gathering, and another for deploying false intelligence to attract members of Al Qaeda into an ambush.[43]

The United States has also developed a plan that was to be put into effect shortly before the U.S. invasion of Iraq, and that would consist of freezing billions of U.S. dollars of Saddam Hussein's bank accounts, amounting to a financial paralysis of the country that would prevent Hussein from purchasing new weapons, and even paying the troops. This plan was halted, however, because of the financial turmoil it could create in the Middle East. This collateral damage was deemed excessive in relation to the benefits of a successful cyber attack.[44] The United States Department of Defense has since worked on defining principles for offensive cyber war, but its efforts seem to be riddled with doubt.[45]

At the same time, some measures have been adopted by the U.S. Military, in creating special divisions to address cyber warfare. For instance, the Air Force has created the 57th Information Aggressor

---

[42] *See* David E. Sanger, *U.S. Steps Up Effort on Digital Defenses*, NEW YORK TIMES (APRIL 27, 2009), *available at* <http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=1&adxnnl=1&adxnnlx=1253975270-G+kOz52VSudZlgfg7AUxRA> (last accessed September 23, 2009).

[43] *See* FOX NEWS, REPORT: U.S. ALREADY CONDUCTING CYBERWARFARE, *available at* <http://www.foxnews.com/story/0,2933,518259,00.html?loomia_ow=t0:s0:a16:g12:r1:c0.333394:b25402662:z0> (last accessed September 23, 2009). This act, however, can be classified as perfidy, which is a clear violation of the principles governing the conduct of warfare. *See also* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. ILJ 179, 202-207 (2006). Regarding Brown's contribution, his draft proposal for an international instrument is particularly relevant, especially Article 23, which reads as follows: "Art. 23. The use of information systems to invite the confidence of an adversary to lead it to believe that an individual, location, or facility is entitled to protection under the law of armed conflict, with intent to betray that confidence, constitutes perfidy, and States shall be forbidden from engaging in such acts."

[44] *See* John Markoff and Thom Shanker, *Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk*, NEW YORK TIMES (AUGUST 1, 2009), *available at* <http://www.nytimes.com/2009/08/02/us/politics/02cyber.html> (last accessed September 25, 2009). A vey similar strategy was devised during the invasion of Kosovo, and also halted because deemed illegal. U.S. Department of Defense legal counsel also found that the general rules of international armed conflicts would apply to any cyber operation, and it was based on these rules that they decided for the illegality of the freezing of Slobodan Milosevic's bank accounts. For this report, *see* MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 258 (2007).

[45] *See* U.S. JOINT CHIEFS OF STAFF, QUESTIONS ABOUND IN CYBER THEATER OF OPERATIONS, VICE CHAIRMAN SAYS, *available at* <http://www.jcs.mil/newsarticle.aspx?ID=106> (last accessed September 23, 2009).

Squadron, based in the Nellis Air Force Base (Nevada), and the Army has created the Network Warfare Battalion.[46]

In June 2009, the UK government released a report on cyber security, reaching essentially the same conclusions as the U.S. report, in the sense that the UK also believes itself to be underprepared for the event of a cyber conflict, and it highlights the need for international cooperation on the matter.[47]

The North Atlantic Treaty Organization (NATO) has also stepped up to discuss the issue of cyber warfare. Triggered by the attacks against Estonia in 2007, the Cooperative Cyber Defense Center of Excellence (CCDCOE) was created in Estonia in 2008, receiving shortly thereafter the status of International Military Organization before NATO.[48] This young institution has engaged in discussing the legal implications of cyber warfare (most notably with a Conference on the topic in September 2009),[49] but it has so far failed to offer concrete results.

Talk about the regulation of cyber warfare has also been initiated at the United Nations level by the request of Russia in the late 1990s, but so far there have been no significant developments.[50]

There have also been attempts in academia to propose regulatory frameworks for cyber warfare. The first proposal is one by a Ukrainian professor, who treats cyberspace as a global common, and that it shall not be used for any ends that are not pacific (much alike the regulations regarding outer space).[51]

The second one is by a former member of the legal counsel of the U.S. Defense Information Systems Agency.[52] This proposal starts by defining "information attack",[53] and mentions the fundamental principles applicable (necessity, humanity, proportionality and chivalry).[54] It also outlines the non-

---

[46] *See* Corey Kilgannon and Noam Cohen, *Cadets Trade the Trenches for Firewalls*, NEW YORK TIMES (MAY 10, 2009), *available at* <http://www.nytimes.com/2009/05/11/technology/11cybergames.html> (last accessed September 25, 2009).

[47] *See* STUART S. MALAWER, CYBERWARFARE: LAW AND POLICY PROPOSALS FOR U.S. AND GLOBAL GOVERNANCE, *available at* <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1437002> (last accessed September 25, 2009).

[48] *See* COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE, HOMEPAGE, *available at* <http://www.ccdcoe.org/> (last accessed September 23, 2009).

[49] *See* COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE, PRESIDENT OF ESTONIA OPENED INTERNATIONAL CYBER CONFLICT LEGAL AND POLICY CONFERENCE, *available at* <http://www.ccdcoe.org/149.html> (last accessed September 23, 2009).

[50] United Nations General Assembly, *Resolution "Developments in the field of information and telecommunications in the context of international security"*, UN DOC. A/RES/53/70, of 4 January 1999. Cited by William Church, *Information Warfare*, 837 INTERNATIONAL REVIEW OF THE RED CROSS 205 (2000), *also available at* <http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/57jqcz?opendocument> (last accessed September 24, 2009).

[51] The original proposal is available at <http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57> (last accessed September 28, 2009). An English translation of the text by Oleksiy Kononov, to whom I am highly indebted, is an appendix to this article.

[52] Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. ILJ 179, 215-221 (2006).

[53] The relevant provision is the following: "Art. 1.a. a. The term "information attack" means the use of computer and/or other information or communications systems to destroy, alter, or manipulate data or images, engage in denial-of-service attacks, transmit malicious code, or perpetrate similar attacks, or do physical damage to any target, for the purpose of inflicting injury or degrading the enemy's ability or will to fight."

[54] The relevant provisions are the following: "Art. 2. This Convention regulates the use of information systems in armed conflict, applying and upholding the generally accepted principles of distinction, military necessity, humanity, proportionality, and chivalry" and "Art. 18. States shall conduct information warfare according to customary international law principles of military necessity, proportionality, humanity, and chivalry. States shall not conduct information attacks in a manner so as to cause superfluous injury or unnecessary suffering."

permissible targets of cyber attacks, drawing heavily on other rules of IHL,[55] and determines the enactment of municipal legislation sanctioning noncombatants who engage in acts of cyber warfare.[56]

The larger part of these policy-level developments, when they even mention the possibility of using private contractors in cyber warfare, seem to mention that the involvement of the business sector is important.[57] They fail, however, to offer and explanation as to why. The indispensability of the connection between the private sector and government in information warfare efforts has not been argued persuasively in the literature on the field.

One of the most commonly advanced arguments is that the private sector is better positioned than the government when it comes to incorporating and responding to fast-evolving technologies.[58] This is part of the general argument in favor of privatization of warfare in general, and is one that can hardly stand on its own. While it is true that the governmental military apparatus of many countries is being gradually replaced by the private sector, this does not necessarily have to do with the ability of the private sector to adapt to change in a quicker pace. Research in the field of political science regarding the operation of private military contractors has shown that they have not necessarily represented a major increase in the evolution of military technique, at least not one that outdoes what the governmental military could have accomplished on its own.[59] There is also the risk that computer systems of private companies will be more vulnerable than governmental computer networks simply because smaller companies do not have the same resources to invest in high computer security as the

---

[55] The relevant provisions are the following: "Art. 12. Information attacks calculated to cause physical damage shall be directed against only targets whose destruction, damage or neutralization confers a definite military advantage, provided that military advantage outweighs the adverse effect on civilians or the civilian population.

Art. 13. Information attacks which are intended or may be reasonably expected to cause widespread, long-term, and severe damage to the natural environment, and thereby to prejudice the health or survival of the population, are prohibited.

Art. 14. In addition to the prohibitions set forth in Articles 12 and 13 of this Convention, information attacks directed against works and installations containing dangerous forces, such as dams, dikes, and nuclear facilities, whose attack may cause severe losses among the civilian population, shall be attacked only if they are used in regular, significant and direct support of military operations, and if such attack is the only feasible way to terminate such support.

Art. 15. Information attacks directed against any of the following facilities shall be prohibited: a. Medical and religious facilities. b. Banks; stock, bond and commodities markets; and any other financial institutions. c. Supplies and distribution systems for food and water, unless the supply or distribution system is used exclusively for providing food and water to lawful combatants. d. Supplies and distribution systems for electricity and other energy sources for the civilian population, unless the systems are used to supply energy to military installations, and the military advantage gained by their destruction, damage or neutralization outweighs the adverse effect on the civilian population. e. Communications systems used by the civilian population, unless the systems are also used by combatant forces, and the military advantage gained by their destruction, damage or neutralization outweighs the adverse effect on the civilian population. f. Sites protected as cultural property. This Convention shall not prejudice the right to attack the above facilities if they are being used to shield other, lawful targets from attack."

[56] The relevant provision is the following: "Art. 31. States shall enact legislation to prohibit noncombatants within its jurisdiction from engaging in information attacks against other States and shall prescribe criminal penalties for the same. States shall take all reasonable and appropriate measures to prevent and punish noncombatants within its jurisdiction from engaging in information attacks against other States."

[57] *See* in particular GREGORY J. RATTRAY, STRATEGIC WARFARE IN CYBERSPACE 363-364 (2001) (part of a long chapter explaining the full evolution of cyber warfare policies in the U.S., and repeatedly mentioning the matter of private sector involvement, but not justifying the need for it).

[58] *See* TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING 174 (2009) (describing the account of one IT specialist hired by the U.S. military who described the technology around him as a "colossal letdown").

[59] *See* P.W. SINGER, CORPORATE WARRIORS – THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 154-157 (2008).

government, a factor that further challenges the idea of greater technical expertise of the privatized cyber military.[60]

Also, the costs of private contractors are not necessarily lower that the ones of a governmental employee. What does happen, especially in the intelligence sector, is that individuals will have great amounts of financial resources invested by the government in their high-level training and, as soon as the training is complete and a high security clearance is obtained, these individuals will leave their jobs with the government only to return to governmental buildings as contractors.[61] Therefore, in this specific case, by creating such favorable conditions to the privatization of warfare, the government is in fact losing the resources it invests in training of high level military and intelligence agents.[62]

Another argument for the privatization of warfare is that the private sector is more often than not the primary target of cyber attacks, and therefore its involvement is inevitable and indispensable.[63] However, an analysis of the principles of IHL applicable to situations of cyber conflict easily ruled out the possibility that the private sector be legitimately targeted by cyber attacks. In fact, if anything the private sector should be clearly differentiated, as computers launching cyber attacks become legitimate targets for cyber and physical attacks. If these computers are located in a commercial building shared with other companies, there is actually a risk of collateral damage on civilian property caused precisely because cyber warfare has been privatized.

One final argument is that the same networks and "cyber highways" are used for civilian and military purposes alike.[64] One 1996 estimate indicated that over 95% of military communications happened over commercial communications systems.[65] While this is an argument that deserves some attention, it does not necessarily justify the privatization of these services. The fact that cyber *security* is public-private by definition does not imply that the cyber *military* should also be public-private.[66] It does call for increased efforts in protecting networks in general, and may perhaps justify closer cooperation in defensive cyber warfare, but it by no means justifies the delegation of offensive cyber warfare capabilities to the private sector.

---

[60] *See* P.W. SINGER, CORPORATE WARRIORS – THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 163 (2008).

[61] *See* generally TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING 28-29 (2009). On the privatization of intelligence services, *see also* Simon Chesterman, *"We Can't Spy… If We Can't Buy!": The Privatization of Intelligence and the Limits of Outsourcing "Inherently Governmental Functions"*, 19 EJIL 1055 (2008); and Simon Chesterman, *Intelligence Services*, *in* PRIVATE SECURITY, PUBLIC ORDER: THE OUTSOURCING OF PUBLIC SERVICES AND ITS LIMITS 184 (Simon Chesterman and Angelina Fisher eds.) (2009).

[62] *See* P.W. SINGER, CORPORATE WARRIORS – THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 76-78 (2008).

[63] *See* Stuart H. Starr, *Toward a Preliminary Theory of Cyberpower*, *in* CYBERPOWER AND NATIONAL SECURITY 43, 65 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009); GREGORY J. RATTRAY, STRATEGIC WARFARE IN CYBERSPACE 328 (2001); and Daniel T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, *in* CYBERPOWER AND NATIONAL SECURITY 24, 41 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

[64] *See* Michael Likosky, *The Privatization of Violence*, *in* PRIVATE SECURITY, PUBLIC ORDER: THE OUTSOURCING OF PUBLIC SERVICES AND ITS LIMITS 11, 17 (Simon Chesterman and Angelina Fisher eds.) (2009) (noting that the internet was created out of a public-private partnership); P.W. SINGER, CORPORATE WARRIORS – THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 100 (2008); TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING 164 (2009); and Thomas C. Wingfield, *International Law and Information Operations*, *in* CYBERPOWER AND NATIONAL SECURITY 525, 535 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

[65] *See* Richard W. Aldrich, *The International Legal Implications of Information Warfare*, *available at* <http://www.airpower.au.af.mil/airchronicles/apj/apj96/fall96/aldricha.html> (last accessed September 24, 2009), also published in AIRPOWER JOURNAL (Fall 1996).

[66] *See* Franklin D. Kramer, *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, *in* CYBERPOWER AND NATIONAL SECURITY 3, 4 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

Therefore, despite policy-level rhetoric aimed at justifying the privatization of cyber warfare as an essential step if sufficient cyber capabilities are to be acquired, there seems to not be a convincing argument justifying privatization as a necessity, rather leaving it as an option. Despite the way in which the rhetoric goes, it seems that the privatization of cyber warfare in countries such as the United States is inevitable, especially if one considers that currently over 70% of the U.S. intelligence budget,[67] along with considerable parts of its general defense budget, are already spent with contractors, which makes the formation of cyber capabilities exclusively within the regular State military a near-impossible task.

The few legislative proposals that exist for the regulation of cyber warfare at the international level are good initial steps. To which extent they can apply to private contractors engaging in cyber warfare, as well as general issues of legal accountability of these contractors, is the topic of the next section.

B. Accountability Issues Regarding the Privatization of Cyber Warfare

Quite a lot has been already discussed on the issue of the privatization of war and the responsibility of States and private military companies for legal breaches undertaken by these contractors.[68] I do not intend to re-open this discussion here in detail, as it would be far beyond the purposes of this paper. However, I will draw on elements so far developed with respect to the general legal scenario as a means to inform the discussion when it comes specifically to cyber warfare contractors, drawing the analogies and making the necessary differentiations, should it be the case.

The instruments being proposed for the regulation of cyber warfare fail to take into account the participation of non-State parties in these conflicts and operations, which has been identified as a major defect in the deterrent effect of these instruments.[69] One exception is the proposal by Davis Brown, discussed above, that proposes a total ban on the uses of private companies for cyber warfare activities.[70]

The available tools for accountability depend naturally on who is called upon to respond for the acts of private contractors. If one wants to call upon the State, then it is imperious to prove that the actions of the contractor were undertaken under command of a State entity. This can give rise to remedies in the

---

[67] *See* TIM SHORROCK, SPIES FOR HIRE: THE SECRET WORLD OF INTELLIGENCE OUTSOURCING 18-19 (2009).

[68] A small sample of the literature can be found on Issue No. 863 of the INTERNATIONAL REVIEW OF THE RED CROSS (2006), which is dedicated entirely to the topic of Private Military Companies, as well as one issue of the EUROPEAN JOURNAL OF INTERNATIONAL LAW, Vol. 19(5) (2008). It has also been the object of a project within New York University's Institute for International Law and Justice. *See* INSTITUTE FOR INTERNATIONAL LAW AND JUSTICE, PROJECT ON PRIVATE MILITARY AND SECURITY COMPANIES, *available at* <http://www.iilj.org/research/PrivateMilitaryandSecurityCompanies.asp> (last accessed September 28, 2009). There is also another project, being conducted by a consortium of universities under the leadership of the European University Institute, on the topic of the legal implications of the use of private military contractors (PRIV-WAR Project). This paper is written in the context of this project. Many working papers related to this topic are available on the Project's webpage. *See* PRIV-WAR, HOME, *available at* <http://priv-war.eu/> (last accessed September 28, 2009). *See also* Alexandre Faite, *Involvement of Private Contractors in Armed Conflict: Implications under International Humanitarian Law*, 4(2) DEFENCE STUDIES (2004), also *available at* <http://www.icrc.org/Web/Eng/siteeng0.nsf/html/pmc-article-310804> (last accessed September 23, 2009).

[69] *See* Tim Stevens, *Cyberwar and Global Law*, *in* UBIWAR – CONFLICT IN N DIMENSIONS, *available at* <http://ubiwar.com/2009/09/05/cyberwar-and-global-law/> (last accessed September 23, 2009).

[70] Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. ILJ 179, 217 (2006). The relevant provision is the following: "Art. 10. States shall launch information attacks from only information systems operated by lawful combatants. States shall not use the information systems of noncombatants or nonparties to the conºict as proxies for such attacks. States shall take reasonable measures to prohibit and prevent such attacks by private persons."

hiring State, or in the State where the attacks happened or of the nationality of the victims (subject to rules on immunity of jurisdiction and enforcement of judgments), or even in a State with which the company or individual undertaking the attack is connected (in which case procedural tools that allow for the State to be named a single or co-defendant must be available).

If one thinks of seeking the company for redress, then it is necessary that States regulate the activities of companies operating within their territories and dealing with cyber warfare. This is one of the requirements of the Cybercrime Convention (Council of Europe),[71] that determines that national legislation be enacted to combat illegal action over the internet that originates from a computer based on the State party's territory.

The applicable legal regimes also have an important role to play in the possibilities for redress. While the application of IHL rules imposes an obligation on States to provide for internal remedies for grave breaches of international humanitarian law (which is the case of an attack against protected property, even if by cybernetic means),[72] it only provides for domestic remedies, there being few (if any) avenues for the enforcement of IHL in international fora, at least in principle.

On the other hand, international human rights adjudicatory and quasi-adjudicatory bodies can address these situations, even if only from the perspective of seeking redress from the State, and not directly from the private actors under State command. If one considers that human rights courts have successfully used international humanitarian law as tools to enhance the application of human rights instruments, IHL can also be an important tool.[73]

---

[71] For a comment on the effectiveness of this instrument regarding cyber security, *see* Clay Wilson, *Cyber Crime*, *in* CYBERPOWER AND NATIONAL SECURITY 415, 430 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009); and Harold Kwalwasser, *Internet Governance*, *in* CYBERPOWER AND NATIONAL SECURITY 491, 515-516 (Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds.) (2009).

[72] The provision on grave breaches common to all Four Geneva Conventions (Articles 50, 51, 130 and 147 respectively), as well as the provision of Additional Protocol I (Articles 11 and 85) state this obligation. The common text is the following: "Grave breaches to which the preceding Article relates shall be those involving any of the following acts, if committed against persons or property protected by the Convention: wilful killing, torture or inhuman treatment, including biological experiments, wilfully causing great suffering or serious injury to body or health, and extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly." The text is different in the Additional Protocol, and has slight variations in the Fourth Geneva Convention, which adds extra elements. Because the Fourth Convention refers to the treatment of civilians, it is also important to add its full text here: "Art. 147. Grave breaches to which the preceding Article relates shall be those involving any of the following acts, if committed against persons or property protected by the present Convention: wilful killing, torture or inhuman treatment, including biological experiments, wilfully causing great suffering or serious injury to body or health, unlawful deportation or transfer or unlawful confinement of a protected person, compelling a protected person to serve in the forces of a hostile Power, or wilfully depriving a protected person of the rights of fair and regular trial prescribed in the present Convention, taking of hostages and extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly."

[73] *See* Hans-Joachim Heintze, *On the Relationship between Human Rights Law and International Humanitarian Law*, 86 INTERNATIONAL REVIEW OF THE RED CROSS 789 (2004); William Abresch, *A Human Rights Law of Internal Armed Conflict: The European Court of Human Rights in Chechnya*, 16 EUROPEAN JOURNAL OF INTERNATIONAL LAW 741 (2005); Amna Guellali, Lex Specialis, *Droit International Humanitaire et Droits de l'Homme: Leur Interaction dans les Nouveaux Conflits Armes*, 2007 REVUE GÉNERALE DE DROIT INTERNATIONAL PUBLIC 539; Noam Lubell, *Challenges in applying human rights law to armed conflict*, 87 INTERNATIONAL REVIEW OF THE RED CROSS 737 (2005); Louise Doswald-Beck and Sylvain Vité, *International Humanitarian Law and Human Rights Law*, 293 INTERNATIONAL REVIEW OF THE RED CROSS 94 (1993); Fanny Martin, *Application du Droit International Humanitaire par la Cour Interaméricaine des Droits de l'Homme*, 83 INTERNATIONAL REVIEW OF THE RED CROSS 1037 (2001); David S. Weissbrodt and Beth Andrus, *The Right to Life During Armed Conflict:* Disabled Peoples' International v. United States, 29 HARVARD INTERNATIONAL LAW JOURNAL 59 (1988); and Liesbeth Zegveld, *The Inter-American Commission on Human Rights and International Humanitarian Law: A Comment on the Tablada Case*, 324 INTERNATIONAL REVIEW OF THE RED CROSS 505 (1998).

There is one hypothesis in which international action can be pursued directly against the contractor, and that is the hypothesis in which the State can sue the contractor internationally for, e.g., overstepping the boundaries of the contract and causing indiscriminate harm, in violation of IHL and human rights norms and the main contract. There has been one case in which a private military contractor has been internationally sued by the State (Sandline by the government of Papua New Guinea).[74] Even though this specific case referred to an issue of payment, matters of violation of IHL and human rights rules can also be the object of arbitration, as long as the respect for these rules is an integral part of the contracts (as they should be).

4. Concluding Remarks

The issue of the regulation of cyber warfare is by itself murky. When one adds the perspective of the privatization of war, yet another rather unclear area of law, there is a double gap in effective regulation. A lot of the currently existing principles of international humanitarian law and human rights law, as well as specific regimes regarding cyber crime, can be applicable by analogy, even though they fail to provide answers to all possible scenarios.

Rules regulating the global commons, especially those on the outer space, also offer some possible source of inspiration, but important differences must be taken into account, potentially diminishing the reach of such analogies. Nevertheless, in the absence of a clear framework, they offer a much needed point of reference.

Specific legislation is, therefore, a necessity in the field of cyber warfare. Emerging proposals have so far largely overlooked the issue of the privatization of this type of conflict, which has been progressively advanced as a policy issue, despite there being no compelling reasons why the privatization of war is a necessity. It is necessary that future regulatory proposals look at the issue of privatization of war, avoiding that indiscriminate cyber attacks occur and affect negatively the lives of innocent civilians and other parties not involved in the conflict. Ideally, the engagement of non-State actors in cyber warfare should be simply prohibited, or State responsibility should be strict, meaning that the State should be engaged by any act of cyber warfare that can be traced back to its territory.

The potentials of technological warfare are increasingly high, and the new domain of cyberspace promises a true revolution in terms of military capabilities. Legislators must, however, impose clear limits on this revolution, so as to avoid unnecessary and disproportionate injury in the name of a type of warfare that may in many instances resemble a video game, but that has a very real and potentially catastrophic reach.

[74] For an account of this litigation, *see* P.W. SINGER, CORPORATE WARRIORS – THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 192-196 (2008). The full text of the contract is an appendix to the book. *Id.*, at 263-270.

Appendix – Proposal for a Convention Regulating Cyberwarfare

Draft by Prof. Merezhko, SJD.

Convention on Prohibition of Cyberwar in the Global Information Network (Internet)

The States parties to this Convention,

BEARING IN MIND the role of the global information network (Internet) in modern communication and economic development of the international community,

CONFIRMING the main principles of the international law including the principle to refrain from using force or threats to use force in international relations as well as the principle of co-operation between states,

STRIVING FOR support of international peace and security and

TAKING INTO CONSIDERATION the development of new information technologies,

EMPHASIZING ON the fact that the global information network (Internet) is the product of activity of the whole mankind,

HAVE AGREED AS FOLLOWS,

Article 1. For the purposes of this Convention the terms shall be used as follows:

a. "Internet" – global information network also known as "Global network" or "World wide web" which represents a global computer network with the information available therein;

b. "Cyberwar" – use of the Internet as well as technological and information resources connected thereto by one state with the purpose to cause harm to military , technological, economic, political and information security and sovereignty of another State.

Article 2. The Internet is the means of technological, information and economic development of the whole international community. It represents a common heritage of mankind which shall not be subject to national appropriation.

Article 3 (Art. 2 RUS). Members of the international community must use the Internet exceptionally with peaceful purposes and in such a way so that it would facilitate strengthening of international peace, security and freedom all over the world.

Article 4 (Art. 3 RUS). The States parties to this Convention shall refrain from the use of Internet as well as technological and information resources connected thereto with the purpose to cause harm to military , technological, economic, political and information security and sovereignty of any State.

Article 5 (Art. 4 RUS). The States parties to this Convention shall reject the use of cyberwar as well as its support in all possible forms in international relations.

Article 6 (Art. 5 RUS). The States parties to this Convention hereby undertake the obligation to introduce in their criminal laws respective norms which would prohibit and prevent cyberwar.

Article 7 (Art. 6 RUS). The States parties to this Convention shall undertake to respect and support creation of the national security systems aimed at prevention of cyberwar.

Article 8 (Art. 7 RUS). The States parties to this Convention shall strive for creation and development of the global security system in the Internet.