2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

Conscription and Cyber Conflict: Legal Issues

Susan W. Brenner
NCR Distinguished Professor
of Law & Technology
University of Dayton School of Law
Dayton, Ohio USA
Email: susanwbrenner@yahoo.com

Leo L. Clarke
R.O.I. Legal Group, Pllc
15 Ionia Ave SW, Suite 510
Grand Rapids, Michigan USA
Email: leo@roilegal.com

Abstract- **This paper examines legal issues that could arise from utilizing a civilian cyber defense corps to defend a nation-state and its assets from cyber attacks. We use Estonia's Cyber Defense League as an analytical device, and we examine issues that may arise under the CDL as it is currently configured and as it might be configured. Our analysis focuses on ten specific issues. We argue that the nature and inherent ambiguity of cyber war will require a reserve corps of IT specialists who can be conscripted if there is a substantial likelihood that a cyber attack will materially disrupt the public order. We also consider the practical and legal aspects of the criteria to be used to select conscripts and factors that will affect the duration of conscription.**

Of course, IT specialists do not work in isolation from the intellectual property and other IT assets owned by their private sector employers. The paper analyzes the issues raised by this symbiosis, including the risk that employers and other owners of assets will be treated as combatants by the cyber attacker, the potential legal issues created by the intellectual property rights of licensors, the potential unintended consequences affecting competition as conscripts defend a competitor of their private sector employer, and the privacy rights of third parties in data necessarily disclosed as part of defense activities. Finally, we consider whether the use of IT assets by conscripts entitles the asset-owners to compensation for the government's taking of their property and whether traditional notions of conscientious objection apply to cyber warfare.

Keywords: conscript, conscription, cyber conflict, cyber warfare, combatant, non-combatant, intellectual property, infringement, conscientious objection, kinetic warfare, Geneva Conventions

I. INTRODUCTION

In an article published in 2010, we analyzed the permissibility of conscripting civilians into a cyber war initiative under United States law [1]. Our premise was that conscription might be necessary if the government could not attract sufficient technological expertise to protect the public interest. Conscription, in other words, would allow the government to obtain the services of IT specialists who declined to assist in defending cyber conflicts because they determined they would be better off in private employment even if cyber attacks were successful.

In this article, we explore the legal and practical issues that are likely to arise when a country embarks on what we refer to as cyber conscription. Our analysis includes not only issues affecting the conscripts but also those who own the IT assets that conscripts would employ in the course of their duties.

We use Estonia's newly-created Cyber Defense League (CDL) as an analytical device [2]. We examine issues that may arise under the CDL as it is currently configured, and as it might be configured. Our analysis focuses on ten issues, each of which is examined below.

II. CONSCRIPTION FOR ATTACK-PREPARATENDESS OR DEFENSE

Since cyber attacks are inherently ambiguous in terms of source, intent, scope and duration, it is reasonable to assume that a cyber conscription program will be anticipatory, i.e., will be implemented before attacks occur or are expected. That brings us to the nature of the attacks: Based on what happened in Estonia in 2007 and in similar attacks, we believe it is reasonable to assume that cyber assaults will be of relatively limited duration, as opposed to the sustained assaults that have characterized kinetic warfare.

We based this assumption on several factors, one of which is that, unlike kinetic warriors, cyber attackers do not have to be physically present on the targeted state's territory; kinetic attacks tend to be prolonged because they are part of a zero-sum struggle to achieve a certain objective, e.g., gain control of territory, and because they are predicated on a mobilization of men and materiél. Cyber attackers operate remotely, and may have very different objectives; an attack, or series of attacks, may be the objective in and of itself. The attackers' goal may simply be to take targeted systems offline for some period of time, to demonstrate their ability to do so and/or the victim state's inability to prevent them from doing so, either of which could undermine the victim state's security.

For these and other reasons, we believe the appropriate model for cyber conscription is an as-needed force -- a version of the "National Guard" or "reserve" forces that are formed and trained before need arises and are "called up" to active

service when the need does arise [1]. As we note below, from what we know of the CDL, it seems to conform to this model.

III. WHEN SHOULD CONSCRIPTS BE ACTIVATED?

The inherent ambiguity of cyber conflict also raises the issue as to the appropriate criteria for activating conscripted reserves. The argument could be made that military forces should not be used for "mere law enforcement" because that is the role of local police. Under this argument, cyber conscripts should not be activated unless there is clear evidence of a nation-state sponsored attack. Unfortunately, experience shows that the actual sponsor and even the source of an attack will remain ambiguous long after the attack has ended. Therefore, a presumption against nation-state involvement would typically render use of conscripts ineffective.

We believe that a better analog is the use of national guards or reserve militia to enforce domestic laws in times of riot and other civil unrest. Activation in these circumstances is justified on the ground that the police force would not able to maintain public order without additional resources. Applying that approach to cyber defense might suggest that the conscript reservists should be activated if there is a substantial likelihood of a material disruption of the public order. For example, reservists would not be activated to defend attacks on non-essential services where the only potential losses are economic – such as an attack on large e-commerce sites, but would be activated where life or health were jeopardized – for example power grids, water supplies or medical facilities.

IV. CONSCRIPT SELECTION AND QUALIFICATIONS

When the U.S. Army drafted Elvis Presley in the 1950s, it was not for his singing voice and when it drafted Muhammad Ali in the 1960s, it was not for his boxing skills. Conscription has historically been a *levee en* masse or a lottery, not a targeted selection of individuals with specialized talents to perform particular functions. That aspect of conscription derives from the fact that until recently, massed manpower was the predominant engine of warfare.

The engines of cyber warfare are very different, which means the selection process must entail much more detail than the typical "draft registration" – name, age, address, education, physical condition and occupation. Conscripting IT personnel would require more detailed information about education and work experience, including familiarity with various platforms, software and industries. This means the selection process would require much more effort and planning on the part of the government and more response effort from the potential conscript.

Since complex IT functions generally require teams of professionals to coordinate their efforts, cyber defense would be most effective if entire "squadrons" were conscripted at the same time. Thus, conscription might be conducted by drafting

the workforce of a particular corporation or government agency. (Even government employees must be conscripted since they would otherwise be free to terminate their employment with the government and avoid service.) As we explain below, depending on how it is structured, such conscription could raise competitive and equitable considerations.

Similarly, the nature of cyber attacks will likely require a certain degree of specialization reflecting the IT structures and practices of specific industries. For example, IT specialists employed by financial institutions are unlikely to have the knowledge to respond to attacks on the electrical grid. Prompt and effective defense would, instead, require conscription of specialists who are responsible for designing and maintaining parts of the grid. Therefore, the conscription program may require more sophisticated organizational structures to ensure that specialized talents can be employed to their highest and best use as attacks affect different industries and locales. For example, command structures might have to adopt non-traditional approaches involving dual reporting according to both expertise and industry experience.

V. DURATION OF CONSCRIPTION

According to reports, the CDL is currently a voluntary "cadre of computer specialists" who will defend Estonia's computer infrastructure [2]. Since the CDL is part of the Defence League, we assume CDL members occupy a status analogous to that of members of the National Guard or reserve forces of other countries. That is, we assume CDL members can be called up to active military service, which in this context would involve cyber conflict.

If that is true, CDL members, like members of analogous units established in other countries, can presumably qualify as combatants under Article 4 of the Third Geneva Convention [3]. That is, members of a CDL-type cyber reserve force (i) will become combatants when they are called to duty and (ii) will otherwise occupy the status of civilian noncombatants [3], [4].

This dichotomous status generally proves unproblematic in the context of real-world warfare. In kinetic warfare, a reservist's status shifts from civilian to combatant when he is called to duty, and persists as long as he is on active duty with the military. The period of active duty is likely to last for weeks, months, even years. There is, therefore, a defined, temporally stable shift from one status to another; the clarity of this shift is enhanced by the fact that the reservist is usually summoned to serve his active duty in a location other than that where he lives as a civilian, is required to wear a uniform (versus civilian clothes) and engages in traditional martial activities.

Like conventional reservists, cyber conscripts will be called to active duty, but the nature and duration of that duty will differ from that of traditional reservists. Logically, there are two ways to structure the activation of cyber conscripts: One is

to activate them when a cyber attack is in progress or is imminent; in this alternative, the period of conscription would be coterminous with the length of the attack or the attack alert. Once the attack, or the threat of an attack, ended, the cyber conscript could be relieved of duty and return to civilian status.

The other option is to have cyber reservists permanently activated, on the not-unreasonable premise that they may need to respond to cyber attacks with little, if any, notice. This option effectively deprives cyber reservists of their civilian status, which we believe means it is neither a viable nor a necessary alternative. We do not see it as a viable alternative because it would presumably mean that members of a CDL-style cyber defense corps were full-time members of the military and, as such, unable to accept civilian employment. The countries that elected to implement this option would, therefore, deprive themselves of the services of an essential cadre of trained computer professionals. Countries bore this burden in other wars, such as World War I and World War II, because they had no other choice and because the conscription had an end point, i.e., draftees served "for the duration of the war" [5]. At this point, it does not appear that cyber conflict will have a determined end point, which means that this model of conscription could continue indefinitely.

We also do not see this model as a necessary alternative: Since activated cyber reservists presumably will not need to don a uniform, travel to a military base, or equip themselves with conventional weapons before they can participate in cyber defense, the situational activation option should be adequate.

Assuming that the reservist/activation model is adopted, the question arises as to how long the individual should be conscripted into reserve status. Given the costs of selection and training, there is a strong argument that conscription should be for a moderate length of time such as five years. Any longer period might be counter-productive because the rapid development of IT technology means that the skill sets required for effective defense will change rapidly. Therefore, the qualifications that led to conscription of a specific professional may not exist after five years, or the professional may have changed careers or specialties so that her skills are no longer needed.

It is also possible that conscription would not end on the expiration of a definite temporal period but on a conscript's termination of specified employment. This would be particularly likely if his conscription arose from his role with a particular employer or his involvement with particular IT assets. Since we presume that conscription is not cost-free to either the government or the conscript, there would be no value in continuing to train and include in defense planning, individuals who would not longer be of service. On the other hand, avoiding continued duty as a conscript should not be too easily achieved, since the rationale for the conscription program is that the government cannot rely on the voluntary cooperation of all individuals with requisite skills.

VI. SOLDIERS WITHOUT ARMS: THE NECESSITY FOR ACCESS TO PRIVATE IT TECHNOLOGY

One of the empirical distinctions between kinetic warfare and cyber warfare is the nature of the conflict: In kinetic warfare, confrontations between the two sides occur at a specific physical place; the forces of the respective parties engage in a struggle from which one side will emerge victorious. The struggle is conducted with conventional weapons, e.g., guns, tanks, explosives, provided by the warring states. The confrontations can, and do, occur on the territory of one of the states engaged in the conflict, but under the modern laws of war, the warring parties must make an effort to shield noncombatants from the struggle.

Cyber warfare is waged in cyber space but can wreak havoc in physical space by targeting components of a nation's critical infrastructure. The weapons used to wage cyber warfare differ from those used in conventional warfare in at least two ways: They do not involve the use of kinetic force; and they tend to be available to the civilian population. We assume that a CDL-style cyber defense force would not be composed of civilians with basic computer skills who would use their personal computer equipment to participate in cyber warfare.

We assume, instead, that because protecting a nation's critical infrastructure will be the primary objective in defensive cyber warfare, cyber defense forces will be composed of professionals employed by organizations that make up that infrastructure. In other words, we assume an embedded cyber defense force, one whose members can be called to active duty to defend the organizations for which they work. It seems reasonable to assume, therefore, that members of a CDL-style force will use the organization's IT systems to defend it.

That would suffice if we were analyzing a system that required infrastructure components to defend themselves, and only themselves, from cyber attacks. We, though, are analyzing a generalized cyber defense system, which presumably means that the employees of Infrastructure Component A would be authorized to use that entity's IT systems to defend it *and* other components of the nation's infrastructure. This generalized system could be executed in several ways. For example, the conscript could use his employer's IT assets to defend the IT according to military orders that differ from or supplement his employer's orders. Or, he could be ordered to defend the assets or business of a competitor of his employer, in effect providing benefits to the competitor at no cost to the competitor. Or he could be ordered to assist in defending unrelated assets because of his knowledge of specific technical issues or his general managerial and organizational skills.

This symbiosis between the human capital furnished by conscripts and the technology required for effective defense raises many complex issues, some of which we will discuss in the following sections.

VII. EFFECTS OF HOSTING CONSCRIPTS: POTENTIAL COMBATANT STATUS FOR INFRASTRUCTURE OWNERS

A fundamental issue is the status under international law the owners of IT infrastructure whose assets are used by cyber defense corps members in responding to attacks. It is likely that most of the individuals or companies that fall into this category will be the conscript's employer. As we saw in § IV, activated members of a CDL-style cyber corps will be combatants under the laws of war. The issue we take up here is whether the same is true of their employers.

Under Additional Protocol I of the Geneva Conventions, civilians lose their non-combatant status "for such time as they take a direct part in hostilities" [4]. Interpretative guidance for this provision says direct participation consists of "specific acts carried out by individuals as part of the conduct of hostilities" between warring states [6]. To qualify, such acts must (i) be likely to adversely the military operations of a party to the conflict or to injury persons or property, (ii) have a direct causal link with the adverse effect or injury and (iii) be specifically designed to cause the effect or injury [6]. Merely producing war materiél does not constitute direct participation, but a conscript's use of her employer's IT assets to defend an attack could be interpreted as not mere production of a weapon, but actual use of the asset as a weapon, even though it is used solely in defense [7].

In other words, a conscript's use of her employer's equipment or intellectual property in the course of carrying out her military orders could cause the employer to become a combatant and therefore a legitimate target for attack. This latter point would be academic if the employer is already under attack, but could present important issues when a conscript uses the employer's assets to defend another entity. And the argument that the employer's role constitutes direct participation in hostilities might be inferentially strengthened by the fact that the employer's authorization to the conscript encompasses the repeated use of the equipment for military purposes.

Another issue that might arise is whether use of an organization's computers might transform non-cyber corps employees who supported the efforts to repel the attack into combatants, on the same premise outlined above.

It is also possible that CDL-style cyber corps members could be activated to defend entities other than their own employers. Logically, this could occur in either of three ways: The CDL members could travel to another site to launch their defensive efforts; they could use their employer's computers to do so; or they could use computers that were in/near their employer's premises but reserved for cyber corps defense activities. The first scenario does not seem practicable if the need to respond is immediate; and if the attacks were part of a sustained series of attacks, this also might not be a viable option. Utilization of the second scenario would presumably raise the issue outlined above, with the additional factor that allowing

use of one's property as a weapon to defend another's property presents an even stronger case for finding combatant status. The third option, thought, would protect the employer from combatant status because using cyber corps-dedicated weapons would not implicate the CDL member's employer in the defense of a third party.

Logically, the "direct part in hostilities" issue could arise for another participant in any cyber war effort: the Internet Service Providers (ISPs). Since we are postulating a civilian-staffed cyber corps the efforts of which are primarily dedicated to defending civilian entities from cyber attacks, it is reasonable to assume that cyber attacks and the cyber corps' responses to attacks will all travel via commercial ISPs. The ISPs' role could, at least arguably, be construed as taking a "direct part" in the cyber hostilities; some have analogized the ISPs' role as the equivalent of using military aircraft to bomb enemy targets.

We are not asserting that the employers and co-workers of entities who employ members of a CDL-style cyber corps categorically become combatants by playing the roles outlined above. Nor are we making a similar assertion for ISPs whose systems carry defensive (and offensive) cyber attack signals. We simply note that the issue can arise in this context, which might make it prudent for a country developing a cyber corps to incorporate that possibility into its planning.

VIII. ECONOMIC CONSIDERATIONS: CONSCRIPT USE OF INTELLECTUAL PROPERTY

The symbiotic relationship between conscript and infrastructure creates another distinction between conscription for cyber defense compared to defense of kinetic warfare. The only requirements for someone drafted into traditional, kinetic military service are that the inductee be healthy, reasonably intelligent and not suffering from a mental disorder. The inductee's particular expertise – if any – is generally irrelevant (though it may play a role in his eventual unit assignment). The government provides all necessary lodging, food, equipment and training necessary to fulfill the conscript's obligations. The cyber conscript, in contrast, is drafted for his or her ability to bring specialized knowledge to bear in supporting the nation's sovereign integrity. That knowledge is likely to include information and ideas that are protected under intellectual property laws.

(We use "intellectual property" in its broadest definition to mean ideas, expressions of ideas and know-how including trade secrets, other proprietary information. These issues are made more complicated by legal doctrines that require an owner of intellectual property to take appropriate action to enforce its property rights at the risk of losing them against other parties.)

A conscript's access to intellectual property can become an issue even if he or she merely uses IT assets owned by the government. Assume, for example, that a conscript's executing orders requires her to use her knowledge of source code or

other proprietary information associated with third party software her employer had licensed. Her employer (or the third-party licensor) could seek to bar the conscript's carrying out her orders on the basis that she would necessarily use its intellectual property in doing so. The argument would be that such a use constitutes an infringement of the owner's property rights.

Rather than simply using licensed software, it is more likely that to carry out her orders, the conscript would need to revise or add code to a copyrighted software program licensed by her employer or another attack target. Such an act would probably constitute infringement, absent an appropriate license. And if the conscript's orders required her to access computers beyond the authority given by her employer, she might well be guilty of a criminal offense.

In short, absent a legislative solution, executing her orders could expose the conscript and the government to liability under intellectual property laws and/or under laws making it a crime to access a computer without being authorized to do so or in excess of one's authorized access. Therefore, in developing conscription legislation, consideration should be given to including a provision that addresses addressing a conscript's authority to use intellectual property licensed by her employer and/or others without paying a fee. The conscription legislation might, for example, grant the government a free, non-exclusive license to use all intellectual property that might be inevitably disclosed in the course of a conscript's service. (Whether this statutory license would constitute a taking is discussed in part X below.) Otherwise, cyber defense could be impeded by uncertainty and even litigation regarding conscripts' rights to use their employment-acquired knowledge in support of the defense effort.

IX. POTENTIAL UNINTENDED ECONOMIC CONSEQUENCES

The use of conscripts and related IT assets might also have unintended economic consequences.

Using conscripted forces to defend against cyber attacks raises one such issue because prudent management practices require governments and businesses to protect their IT assets and data even in the absence of a cyber war threat [8]. In comparison, kinetic warfare typically presents risks fundamentally different from those presented by "business as usual."

For example, the military's use of conscripted soldiers to defend a warehouse from invading forces inures to the benefit of the merchant owner as well as to the public at large. The warehouse is saved from destruction at no cost to merchant owner or his insurers. In those situations, however, the military effort indisputably arises from a risk not incurred in normal business circumstances – an unambiguously hostile attack by a foreign nation-state. Conscripts, on the other hand, may be ordered to defend against an attack that is not "military" in origin, but is "merely" cyber crime or cyber terrorism. (This risk, of course, arises from the inherent

ambiguity of cyber attacks.) The conscript might, therefore, be involved in implementing an IT defense that does not differ materially from defense against cyber crime. In this context, adoption of a conscription program might cause owners of IT to under-invest in IT security.

A different, but perhaps more significant, unintended consequence of conscripting corporate employees to defend cyber attacks is the potential conflict that might arise if conscripted employees of one organization were given access to another organization's IT assets or data to defend an attack. Since most IT systems are exceedingly complex and proprietary in nature, it is only reasonable to expect that the conscripts would have to work with employees of the target organization, and would have access to proprietary information concerning the target's customers, suppliers and other vendors. For example, assume that conscripted employees of Bank A were ordered to assist in the defense of an attack on Bank B, a competitor, and to mitigate resulting damage to the financial system. In the course of executing their orders, the conscripts might (i) disclose information Bank A had acquired at great cost to employees of Bank B, (ii) learn about strengths and weaknesses of Bank B's systems, (ii) be exposed to confidential pricing and other information granted to Bank B by vendors to both banks, and (iv) receive access to financial information of Bank B's customers which is protected by privacy laws.

Such a situation would not be acceptable to any of the affected parties. Bank A would not appreciate its competitor's receiving the benefit of its investment. Bank B would complain about the disclosure of its proprietary information. The vendors would allege a breach of confidentiality rights, and customers would allege breach of privacy laws. None of these consequences is a necessary result of the cyber attack; each is a real and likely substantial cost; and collectively the resulting harm may exceed that of the attack itself.

One response to these unintended consequences may be to preclude conscripts from communicating directly with competitors and instead require screening procedures. However, screening and similar procedures that required the insertion of third parties would introduce additional levels of complexity, delay and expense into situations that require immediate and efficient response.

X. COMPENSATION

As we explain below, compensation issues arise both for conscripted individuals and for third parties involved in a cyber conflict event.

Conscripts generally receive compensation from the military and forego the income from their pre-conscription private employment; this is considered to be a cost of citizenship. Reservists are typically paid at military scales while activated, although some employers may continue to supplement their compensation as a form of social responsibility.

There is, of course, a risk that an employer will terminate a conscripted employee because its business needs will continue to require services even if an attack occurs. Termination in this context is unlikely, however, because of the shortage of skills in the market place, the probable short activation period, the training and other transaction costs involved, and the likelihood that the replacement would also be conscripted. In light of these factors, it would not appear that either efficiency or equity would require special compensation provisions for conscripts.

The discussion above noted several situations in which a conscript's performance of his duties may cause his employer and/or third parties to incur costs or lose the benefits of bargains. These losses would result from the practical relationship between conscripts and IT technology typically owned by employers and those other entities. Given those financial consequences, owners of IT assets used by conscripts or infringed upon in the execution of orders might seek compensation from the government.

Estonia's Constitution, like the constitutions of many other countries, prohibits the government from taking private property unless the taking is in the public interest and for fair and immediate compensation. The taking or destruction of property in the course of warfare, however, is generally not considered to be a "taking" for such constitutional purposes [8]. Moreover, an asset-owner would not seem to have an equitable claim for compensation when the conscript is defending the owner itself.

On the other hand, the complexities of intellectual property law and the technology involved may counsel, as suggested above, including in the conscription legislation, an explicit grant of non-exclusive licenses to the government either at no cost or at a cost to be determined after the use is completed. Such explicit treatment would tend to reduce doubt, confusion and litigation and set the framework for consensual resolution of the appropriate amount of compensation that the government should pay for its requisition of assets for the war effort.

XI. CONSCIENTIOUS OBJECTION

Like many other countries, both Estonia and the United States recognize the right to refuse to serve in the military "for religious or ethical reasons" [9], [10]. If these or other countries decide to implement a conscript-style cyber corps, the issue of conscientious objection may arise. Since a cyber corps conscripts civilians into military service, the basic legal premise for conscientious objection seems to be established in this context. An issue may arise, however, as to whether conscientious objection is appropriate in conscription for cyber warfare.

Historically, conscientious objection was primarily based on religious or philosophical objections to the "obligation to use lethal force" [11]. While it is certainly possible that cyber attacks could result in a loss of life, the nature of cyber

combat is notably less lethal than kinetic warfare. This might, or might not, result in a lesser incidence of conscientious objection in this context. It also might, or might not, require countries to determine how traditional principles governing conscientious objection apply to cyber warfare.

XII. CONCLUSION

Our purpose in writing this paper is to identify many – but undoubtedly not all – of the legal issues that are likely to arise when a country elects to implement a CDL-style civilian cyber defense corps. Certain of the issues that will arise in a particular instance will, at least to some extent, be specific to the laws of that nation-state. Based on our research, though, we believe many of the issues are likely to be consistent, at least in countries that clearly demarcate civilian and military spheres of operation. It may be possible to address the more generic issues with international agreements or, perhaps, a template of model laws similar to the Toolkit for Cyber crime Legislation developed by the United Nation's International Telecommunication Union [12].

REFERENCES

[1] S.W. Brenner & L.L. Clarke, "Civilians in Cyber warfare: Conscripts," in Vanderbilt Journal of Transnational Law, vol. 43, (4), 1011, 2010.

[2] H. Kenyon, "Volunteer Cyber Corps to Defend Estonia in Wartime," Defense Systems, January 12, 2011.

[3] Geneva Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 75 U.N.T.S. 135.

[4] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) Article 50, June 8, 1977, 1125 U.N.T.S. 3.

[5] Ex parte Billings, 46 F.Supp. 663 (U.S. District Court for the District of Kansas 1942).

[6] Assembly of the International Committee of the Red Cross, Interpretative Guidance on the Notion of Direct Participation in Hostilities 995 (February 26, 2009).

[7] Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 619 (Yves Sandoz et al. eds. 1987).

[8] S.W. Brenner & L.L. Clarke, "Civilians in Cyber warfare: Casualties," in Southern Methodist University Science & Technology Law Review, vol. XIII, (2), 2010.

[9] Constitution of the Republic of Estonia, Article 124(2).

[10] Welsh v. United States, 398 U.S. 333 (U.S. Supreme Court 1970).

[11] Special Rapporteur on Freedom of Religion or Belief, Framework for Communications: Conscientious Objection, Office of the United Nations High Commissioner for Human Rights.

[12] United Nations, International Telecommunications Union, ITU Toolkit for Cyber crime Legislation, 2010, http://www.itu.int/ITU-D/cyb/cyber security/projects/cyber law.html.