# Towards a Global Regime for Cyber Warfare

Dr Rex HUGHES
*Cyber Security Project, Chatham House, London*

**Abstract.** With two years having passed since the infamous cyber conflict between Estonia and Russia, international society still lacks a coherent set of principles, rules, and norms governing state security and military operations in cyberspace. For parties committed to promoting the cause of peace and stability in a multipolar world, this is a troubling notion since history shows that the likelihood of a new arms race is high when disruptive technologies dramatically alter the means and methods of war. As more nations aspire to project national power in cyberspace, a new digital arms race appears to be imminent if not already upon us. Thus, there is a central question confronting international society and more specifically the diplomatic community in cyberspace: What steps can be taken both today and into the future to forestall a major arms race and interstate competition in cyberspace? In order to begin addressing this complex question from the perspective of the Euro-Atlantic Community, this paper discusses both the challenges and opportunities of regulating 21st century cyber warfare. The paper is divided into three sections. Section 1 examines the evolution of the laws of armed conflict (LOAC) since the late 19th century. Section 2 examines how the LOAC apply to cyber warfare as viewed primarily from a US perspective (since US scholars have dominated the international regime discourse thus far). Section 3 examines what is needed to create a global regime for cyber warfare and specifically the role that NATO and the Euro-Atlantic Community can play.

**Keywords.** Law of Armed Conflicts, Cyber Warfare, Revolution in Military Affairs, Global Regime

> *Because the entire law of war regime has been built upon a Westphalian foundation, the transformative properties of cyber warfare are just as breathtaking. We are left pondering some fundamental questions - what constitutes force? What is a hostile act? When is self-defense justified in response to a cyber attack? Is the use of traditional means of force ever justified in response to a cyber attack? These are not easy questions and the international legal regime is lagging far behind the problems presented by the increasingly sophisticated technological possibilities in this area.*
>
> --Lt. Col Jeffrey K. Walker[1]

## Introduction

When viewed systemically, the current generation of cyber weaponry demonstrates an enormous potential to alter the means of hostile attack and in turn of response. While our 21st century armed services are adjusting to the revolution in military affairs (RMA), the broader community of business, transportation, energy, research, health, academic, and social services look to their national leaders to provide plans and to conduct operations that will protect their domain of cyber space. Cyber defense for those old enough to remember may call to mind the home front nuclear alert drills plus the bunkers or bomb shelters constructed in the post WWII decades. In cyberspace both military and civilian networks are potential targets.

Overarching questions confront us: What is the current state of cyber warfare when viewed from an international affairs perspective? What options are available to policy makers that seek to fashion a global regime to govern 21st century cyber warfare? And more specifically to the theme of the first NATO CCD COE cyber war conference, what role can an international military alliance such as NATO play in advancing such a regime?

Since the enormous attack on Estonian digital networks, governments around the world have ordered their respective military branches to develop new offensive and defensive cyber capabilities. Some states have even gone as far as to create national cyber command authorities, as is evident in the United States [2]. However, as the attacks mount and more advanced 'cyber weapons' are introduced to the digital battlefield, there is little certainty or international consensus on the rules, or lack thereof, for governing modern cyber battles or larger warfare. Air Force Gen. Kevin P. Chilton, the head of U.S. Strategic Command (STRATCOM) issued a statement in May of this year that 'The Law of Armed Conflict will apply to this domain'[3]. STRATCOM defends the Pentagon's Global Information Grid at home and abroad through its Strategic Command Joint Task Force-Global Network Operations (JFT-GNO). Attempted penetrations of public and private systems number in the tens of thousands a day. As a commander who provides information for decisions by the US President and the Secretary of Defense, Gen. Chilton said that all combat options should be on the table for a US response to a cyber attack. He noted that many attacks thus far have been for the purpose of espionage, and that there can be an argument about the 'semantics of attack versus espionage and intrusion' [4].

## 1. REGULATING WARFARE

### *The Principles and Norms of Armed Conflict*

The law of armed conflict (LOAC also commonly referred to as the 'laws of war' or *jus in bello*) as understood today originated in the mid-19th century, as did the humanitarian regulation of conflict and violence.[1] Since their early beginnings these laws applied primarily to interstate conflict as carried out by uniformed armed forces between two or more states. The principles, rules, and norms that guide today's LOAC can be found in a variety of sources: customary law, international treaties, judicial decisions, legal philosophers, and military manuals. Although the customs of the LOAC can be traced as far back to the 15th century medieval Europe, its more modern origins date back to the American Civil War of 1861-1865 [5]. Until that era Dale Stephens and Michael Lewis, note that 'there was no meaningful *jus ad bellum* because the right to resort to force was essentially unchallenged'. The ideals of knighthood in the Middle Ages provided some restraint against certain warfare cruelties [6]. Not until the 17th century was there a systematic legal code on war and peace. The Hugo Grotius

[1] Sections of the LOAC that deals explicitly with civilians are commonly referred to as *international humanitarian law*.

work of 1625, *On the Law of War and Peace* (*De jure belli ac pacis*), was based on the natural law. In the 18th century natural law and the Golden Rule were formulated by Emerich de Vattel in his 1758 work, *The Law of Nations* (*Droit des gens*). It was not until the American Civil War that the laws of armed conflict were codified and adopted by the leading world states. The first Geneva Convention was agreed upon in 1864 and employed the US Lieber Code (US War Department, General Orders No. 100, 24 April 1863) as a baseline. By 1868 in St. Petersburg a treaty, as noted below, was signed by leading nations/empires (excluding the US) that concerned regulating warfare methods and means.

Regulation of war and violence under humanitarian principles arose in 1863 with the establishment of the International Committee of the Red Cross (ICRC). During the 1876-1878 Russo-Turkish War the Ottoman Empire established the Red Crescent and there followed mutual agreement for respect from both sides whether honoring the principles of the Red Cross or the Red Crescent. The ICRC acts as a guardian and promoter of international humanitarian law.[2] The establishment of the First Convention of the Geneva Conventions in 1863 followed the formation of the ICRC and concerned the welfare of the wounded, civilians, shipwrecked, and prisoners of war. Four Conventions were adopted/revised through 1949. Amendment protocols about victim protections were added from 1977 through 2007. In 1899 and in 1907 peace conferences were held in The Hague for the purpose of regulating weapons in war and the customs and laws of war. The Geneva Protocol to the Hague Convention of 1925 prohibited other uses of gas and biological weapons. Later treaties of 1972 and 1993 covered the production, storage, or transfer of these weapons. A 1951 UN Convention Relating to the Status of Refugees covered post-WWII European refugees and was expanded in 1967 to cover other refugees without time or geographical limitation. While also referred to as the 'Geneva Convention' this UN treaty is actually not part of the Four Geneva Conventions [7].

### *New Weapons and LOAC*

It was not until the 1868 ratification of the St. Petersburg Declaration that emerging military technologies were subject to any type of international legal review. This action is officially stated as the Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight. A rash of new weapons introduced during the American Civil War, including armoured warships, submarines, as well as land mines, machine guns, projectiles filled with clear glass or explosives, exploding bullets, and dumdum bullets designed to flatten on impact. Weapons that caused unnecessary physical harm prompted delegates at St. Petersburg to issue a statement on this vexing issue in their declaration:

> *The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view*

[2] The ICRC explains its mission as 'an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of war and internal violence and to provide them with assistance'. The organization 'endeavors to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles' [8]. The seven Fundamental Principles of the International Committee of the Red Cross are: humanity, impartiality, neutrality, independence, voluntary service, unity and universality. It was not until 1929 with the amendment of Geneva Convention (Article 19) that the Red Crescent was officially recognized as part of the ICRC.

> *of future improvements which science may effect in the armament of troops, in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity.*[3]

In 1977, Protocol 1 of the Geneva Convention also cited the need to carry out international reviews of new weapons. The intent of Article 36 is to determine the lawfulness of new weapons before they are developed, acquired, or incorporated into a military's arsenal. Legal experts have also argued that scrutinizing the legality, means, and methods of new warfare is so basic that it applies to all nations, even those not a party to Protocol 1. Thus, states following international law must ensure that new innovations do not run afoul of international obligations. Article 35 states:

> *In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.*[4]

Article 6 is complemented by Article 82 of Additional Protocol 1, which requires that legal advisers be accessible at all times to battle commanders and that 'on the appropriate instruction to be given to the armed forces on this subject'. Thus, the basic aim of both the St. Petersburg Declaration and Protocol 1 of the Geneva Convention is to ensure that armed forces will carry out battlefield hostilities in strict accordance with the principles, rules, and norms as established by the LOAC. However, one problematic area is found in Article 36 that does not delineate specific means by which legal review of new weapons and methods of warfare will take place, leaving actual practice open to much interpretation. Few states have actually codified this mandate into state practice except for the United States and Sweden.[5] In 1999 the 27th conference of the International Conference of the Red Cross and the Red Crescent encouraged states to, 'to establish mechanisms and procedures to determine whether the use of weapons, whether held in their inventories or being procured or developed, would conform to the obligations binding on them under international humanitarian law'.[6] In 2003, in light of war in the Middle East, the ICRC reaffirmed this goal 'the legality of new weapons under international law' and 'in light of the rapid developments of weapons technology and in order to protect civilians from the indiscriminate effects of weapons and combatants from unnecessary suffering and prohibited weapons'.[7]

[3] Excerpt taken from the section renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, St Petersburg, 29 November / 11 December 1868.

[4] Article 35, Protoco1, 1977

[5] The United States and Sweden both established formal review practices as early as 1974.

[6] Section 21, Final Goal 1.5 of the Plan of Action for the years 2000-2003 adopted by the 27th International Conference of the Red Cross and Red Crescent, Geneva, 31 October to 6 November 1999.

[7] Final Goal 2.5 of the Agenda for Humanitarian Action adopted by the 28th International Conference of the Red Cross and Red Crescent, Geneva, 2-6 December 2003 [hereinafter Agenda for Humanitarian Action].

## 2. LOAC in Cyberspace

Thus far, there is no international consensus on the application of the laws of armed conflict to 21st century cyber warfare, likely irregular warfare. This problem stems from both the loose definition of cyber warfare as well as the lack of precedent through which to guide present and future law. Another challenge is that not unlike other means of 21st century warfare, cyber warfare is coming of age in an era where the Westphalian state order is undergoing vast transformation. As the borderless realm of cyberspace both ignores and challenges state boundaries, a hands-off policy may disrupt or worsen cross-border transactions. As explained by Vida Antolin-Jenkins, USN JAGC (United States Navy-Judge Advocate General Corps), 'Cyberspace operations for the most part do not meet the criteria for 'use of force' as currently defined by international law. Defining the parameters of proportional response through analogy is possible, but creates clear dangers of definitional creep into other areas of international relations that have long been the subject of long and contentious debate' (Antolin-Jenkins 2005: 134). Let us remember that Gen. Chilton does not rule out responding with kinetic force to a cyber attack [2].

*Disruptive Technologies on the Battlefield*

Throughout history, there are numerous examples of disruptive technologies that have changed the way war has been waged, often resulting in enormous transfer of powers. Since hunter-gatherer tribes first wandered the earth, man has sought strategic advantage through the development and application of new technology. William Owens (US Admiral-Ret.), applying historian Martin van Creveld's divisions of military history, reminds us that the 'Age of Tools' (prehistoric age to about 1500 AD) witnessed battles of the 'muscular power of men and animals' using 'the wheel, the stirrup and iron weaponry'. In the 'Age of the Machine' (18th thru the 19th centuries) artillery weapons were eventually wielded by large units of fighting men [9]. The 'Age of Systems' developed between WWI and WWII with radar, long-range aircraft and radio coordinated ground-to-air attacks. We are presently living in a 21st century 'Age of Automation' where even older munitions and aircraft are deployed by sophisticated communications technologies as faster and more precise navigation and related digital devices are currently in development [9].

Using information and/or computer technology to impose one's will upon an enemy is a form of warfare-- information warfare (IW). In 1995 Martin Libicki of the US National Defense University in classifying IW forms stated: 'Seven forms of information warfare vie for the position of central metaphor: command-and-control (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare (PSYW), hacker warfare, economic information warfare (EIW), and cyberwarfare' [10]. Robert Hanseman in the late 1990s anticipated how information warfare will blossom into a full-fledged "Revolution in Military Affairs" (RMA) [11]. Looking specifically to the US global role, Owens sees this RMA as an 'opportunity to use the new information technology to change the very nature of our military, in a way that could reinvigorate American political, diplomatic, and economic leadership in the world for decades to come'. From a specifically US security perspective, Owens holds that in this new century the 'changing world demands a new way of looking at war and the proper military force' [9]. This paper maintains that in addition to this needed military strategy transformation there needs to be a new legal/treaty framework defining the cyber security regime.

Another question: What is the nature of the *force* deployed by cyber attackers or cyber terrorists and is this *force* an act of war? Michael Schmitt points to an International Court of Justice (ICJ) finding that ‘supports a conclusion that a use of force need not be kinetic in nature’ when the ICJ ruled (1986 Nicar. v. US) that ‘although the funding of guerrilla forces was not a use of force, arming and training them was’ [12]. Today cyber weapons may potentially be in the possession of varied and mixed-motive warriors, terrorists, or civilians. The legal assessment of cyber attack or cyber war, Schmitt offers, will come from the community. He concludes that a ‘cyber attack that causes significant human suffering or property damage is obviously an armed attack justifying a response under the law of self-defence. Schmitt also speaks to the need for the law to mature since the ‘global community finds itself at the cusp of normative change’ in seeking a definition of aggression [12]. As this paper urges, the year 2009 is the time to begin constructing a global cyber security regime to bring clarity to the place of cyber attacks or cyber terrorism within the 1945 UN Charter.

### *Info Age Warfare*

The transition through the phases of information technology with increasing dependency upon sophisticated devices and digital applications have led logically to phases --warfare involving information systems, hence new battlefields or rather, *battlespaces*. In one sense, modern information warfare can be traced back to the introduction of long-distance telecommunications. With the introduction of the telegraph, telephone, and radio, both civilian and military leaders gained an unprecedented command and control authority over troops movements and deployments. With a real-time link established between civilian and military headquarters, political leadership where possible could exert much more decision making authority, sometimes to ill effect. US President Abraham Lincoln was the first commander in chief to use the telegraph to issue orders to his Northern Generals in real-time. From across the Atlantic, Queen Victoria made extensive use of the telegraph to communicate her vision to overseas colonial viceroys.

During WWI, communications instruments were fully integrated into land, sea, and air campaigns. Later the sheer complexity and scale of WWII increased the need for cybernetic controlled weapons. As firepower increased again throughout land, sea, and air, the need for more precision and predictability increased. This was especially true in two areas of artillery and air combat. The Bletchley Park British code-breakers of WWII decrypted over 3000 daily German Enigma messages through the computational developments of Alan Turing [13]. The British and US through technology exchanges perfected their microwave and radar system and eventually were able to jam the German radars.

The atomic age only increased cybernetic development as the need for even more precise, reliable, and speedy command-and-control operations increased several orders of magnitude. The deployment of nuclear weapons required the most sophisticated air and space communications networks ever developed. Between the 1950s and 1960s, the space and nuclear race helped propel a host of new information communications technology (ICT) breakthroughs with the invention of the transistor and the microprocessor. From the 1970s forward, many of these dual-use military and space technologies found their way into the civilian sector. Historically, with each generation, the ability to hunt and destroy has increased.

### *Peace and Security and the Cyber Challenge*

'A war of aggression is a crime against international peace. Aggression gives rise to international responsibility' states the UN Charter (Article 5, Paragraph 2 of the Definition of Aggression). This statement provides a basis for considering an attack on the information infrastructure of a nation as an act of aggression. Attacks have the potential to disrupt a nation's power grids, transportation links, health care service, emergency response, financial flows among many other venues. Under this Charter from 1945, a nation has the right to self defence. Lawmakers, diplomats, and military strategists need to confront the tasks for defining and framing the regime that will protect the cyber security for national defence and civil society functions. A major international military alliance such as NATO has a task suitable to its own mandate or charters in harmonizing accepted policy on aggression and protective national defence on the its own membership soil and their protectorates and in its global expanse of cyberspace.

Antolin-Jenkins sums up the predicament of a digital society: 'The strategic and economic power of the increased information awareness and connectivity are coupled with a hugely increased vulnerability to destruction and attack. This information network has created a new battleground'. She also reminds her readers that 'One estimate is that 95% of military information traffic utilizes civilian networks at some stage of communication' [22][14]. How or when could there be a separation of military from civilian networks? Is an attack on a military network also an attack on civilians, or *visa versa*? An advisor to the director of US national intelligence, Steven Chabinsky, reminds us that even if the laws of war 'would forbid targeting purely civilian infrastructure' we need to consider that 'terrorists, of course, don't limit themselves by the Geneva Conventions' [15].

### *Humanitarian Law for Cyber Weapons?*

Does cyber warfare fall under the international humanitarian law (IHL)? Jeffrey Kelsey holds that IHL 'should evolve to encourage the use of cyber warfare in some situations and provide states better guidance in the conduct of these attacks' [16]. He argues that for a decade or more the 'potential threat and opportunity of cyber warfare' have confronted military planners while the 'international community has yet to reach consensus on the application of IHL'. This lack of consensus may be due to a variety of reasons, from holding that the 'current IHL framework can be applied to cyber warfare by analogy' to the realization that vast growth and fluidity of technology would make potential international agreements obsolete [16]. Kelsey further maintains that 'IHL applies to cyber warfare by analogy but contends that IHL must evolve to accommodate and, in some cases even encourage cyber warfare over conventional methods' [16].

The movement in a cyber attack across a neutral state becomes more than a 'mere communication signal', for cyber weapons can cause damage to states as have more conventional weapons. A weapon the 'size of a electron' could be a violation of the territory of a neutral state according to the Hague Convention that 'forbids the movement of weapons' across a neutral state which risks being drawn into a wider cyber conflict when its Internet nodes are engaged by a belligerent [16]. What obligations would a neutral state have as a conduit for cyber attack and mischief? Kelsey argues against establishing new treaties and in favour of states and their military commanders to follow established legal principles in cyber combat [16]. The question remains: What standards should emerge for a cyber security regime under established peace and war legal principles? Since cyber warfare is still in its infancy, some would argue that regulating it is a difficult if not an impossible challenge. However, the so-called *catastrophic* cyber attack is to be avoided, it would be foolish and impractical not to establish some type of international rules of the game as deterrence.

## 3. Towards a 21st Century Global Cyber Regime

Thus far, the diplomatic community has had little to say about the governance of cyber warfare. Two exceptions of major importance include former diplomats with knowledge of ICT have in recent months discussed with this author the major international relations quandaries from cyber threats and attacks plus their own concerns about diplomatic-level solutions. These former envoys are retired senior US Amb. Thomas Pickering who served over four decades in major posting for the US Dept of State, and Amb. David Gross, U.S. Coordinator for International Communications and Information Policy 2001-08. The latter observes that diplomatic silence may be attributed largely to a generational gap and a lack of technical understanding by policy makers since the Internet and associated networks are fairly recent developments; therefore, cyber security concepts in international affairs are still a nascent on the part of the diplomatic community (Gross to the author: April 2009). With wide-ranging diplomatic and corporate experience, Amb. Pickering sees an even larger problem in that forming an international treaty involves major, prolonged steps and major questions: What is the problem to be solved? How will the problem evolve in the future? (Pickering to the author: July 2009). Since cyber warfare is being conducted and developed during a period of wide interstate trade and general economic accord or agreement, there is an opportunity to design a governing framework before an actual global catastrophic attack takes place. Today the questions remains: Can governments be motivated to take action now before it is too late?

Special regimes have been formed for far-ranging interests or activities, such as treaties governing the Arctic, Antarctic, canals, international rivers, and outer space. While somewhat vague or undetermined there appears to be a consensus that outer space begins where airspace ends [17]. Examples of the treaties governing outer space include those governing the International Space Station (1998), Registration of Objects Launched into Outer Space (1975), INTELSAT or International Telecommunications Satellite Organization (1986), INMARSAT or International Maritime Satellite Organization (1976), as well as the ITU or International Telecommunications Union (1932; 1947 as UN agency) [17]. You may ask, ‘Where does cyberspace begin?’ It would appear that cyberspace begins with the keystroke to log on to a cyber network, whether from a mega terminal, a PC, a game console, or a mobile telephone.

Eventually, the ultimate venue for cyber warfare governance would be The Hague as the home of the world’s first Peace Conference and for over a century as the international centre of justice and arbitration, as well as warfare governance. The Hague hosts several international organisations, including the UN International Court of Justice, the Permanent Court of Arbitration, the NATO Consultation, Command and

Control Agency (NC3A). As cyber warfare moves to the forefront of more government agendas, more questions arise as to how the Law of Armed Conflict and the Geneva Convention apply to cyberspace. Responses are likely to range on both sides of the fault line: those who see cyber warfare as fitting neatly under existing LOAC (as well as under the UN charter), and on the other side, those who see the need for an entirely new set of international laws and treaties to govern cyber warfare.

### *A Way Forward*

While it is unlikely that these two countervailing diplomatic/legal views will be reconciled anytime soon, the time is now to begin having this debate in a more serious, focused manner. Again, because cyber warfare is a complex and dynamic issue, these debates will need to be hosted in many different venues and viewed from many different perspectives. NATO is already playing an important role in this debate by hosting conferences such as this June 2009 Tallinn gathering bringing together the relevant players from both member states and global partners. For the foreseeable future, this NATO Center of Excellence can play a critical role in bringing together the best experts both to analyze and to debate the problems from a number of unique cultural and disciplinary perspectives.

As the world's premiere military alliance, NATO is positioned to play a major role by facilitating significant interstate dialogue between civilian and military planners. Each year NATO hosts various fora where such engagements take place. The NATO Global Partnership Program provides a mechanism to reach out to other countries. NATO could also explore reaching out to other peace and security alliances, such as ASEAN Regional Forum (ARF) and the Shanghai Cooperation Organization (SCO), for the purpose of exploring confidence-building measures with that global hemisphere.

Although presently cyber warfare/defense is largely an ungoverned affair, the UN leadership has already acknowledged the severity of the problem and the need for governance. UN secretary-general Ban Ki-moon earlier this year announced that the UN Advisory Board on Disarmament Matters is to include cyber weapons in its arms list [18]. In his prepared February remarks to this Advisory Board the Sec-Gen stated:

> *This year you will be considering cyber warfare and its impact on international security. As you know, there have been many widely reported breaches of information systems in recent years. With both the public and private sectors growing increasingly dependent on electronic information, your work in this area is very timely. It will also complement the efforts of the panel of governmental experts that will be addressing information security later this year [19].*

The UN's International Telecommunications Union last year concluded its agreement with the International Multilateral Partnership Against Cyber-Terrorism (IMPACT) to conduct the ITU Global Cybersecurity Agenda (GCA) with headquarters in Cyberjaya, Kuala Lumpur. The GCA seeks international cooperation for governments, international law enforcement authorities, the private sector, international organisations, and civil society for the purpose of a secure cyberspace. Through five areas the GCA if focused on strengthening the legal framework, technical measures, organizational structure, capacity building, and international cooperation. [20] At its Cyberjaya headquarters inauguration the ITU-GCA was billed as 'public-private initiative' and a 'framework for cooperation aimed at finding strategic solutions to boost confidence and security' in a networked world [21].

Relevant committees beyond the UN should also begin to debate a proper a framework for cyber warfare while other international fora can and should play a role. Significant organisations such as the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Society (ISOC) are positioned to use their technical legitimacy and their soft power to press forward with best practices for member states to follow in securing their own sovereign cyberspace. World Trade Organization (WTO) signatories should develop an agreement for pledges from nations not to promote or solicit mercenaries, or attack a member state's trade infrastructure. On the military side, the national leading military services should be encouraged to act with transparency where possible so as not to launch initiatives that unduly contribute to unnecessary cyber arms race between states.

One of the most difficult governance areas to reconcile will be in the area of police vs. military involvement in cyber security/defence. As the US-led global war on terror has shown, there is no clear line of authority when defending against threats where state involvement is murky at best. Due to the anonymous and secretive nature of cyber warfare, state involvement is often tricky for producing fool-proof forensics that can prove state involvement. While each country will ultimately need to sort through this problem in accordance to its national laws and constitutions, more global debate will be needed to clarify these issues.

Participants in Tallinn are witnesses to the positive leadership role assumed by Estonia and leading to the NATO CCD COE here at the scene of the first acknowledged, major interstate cyber conflict. There is potential for a cyber treaty to emerge should the North Atlantic Council embrace thoroughly the cyber warfare issue and engage the NATO Consultation, Control and Command Agency (NC3A) and the NATO Military Authorities (NMA). The Tallinn cyber convention questions and discussions are a start, but a protocol or treaty governing the conduct of cyber warfare needs serious consideration.

## 4. Conclusion

While cyber warfare is not an entirely new area of modern warfare (at least as viewed within an Internet world), its current evolution poses many challenges to international peace and stability. The increasing quantity and quality of online attacks threaten many parts of civil society that depend on reliable networks and information systems. Growing evidence of state-sponsored cyber attacks is especially alarming and could spark a serious arms race in cyberspace. Understandably, a number of countries have announced plans for full spectrum military cyber commands. As history has demonstrated, while international law cannot stop states from going to war with one another, it can go a long ways towards regulating their conduct should hostilities boil over into actual war. Some may argue that because cyber warfare is still in its formative stages, it is premature to begin work on a global regime to regulate it. However, it can also be logically argued that absence of some rules of the game, states will not feel constrained to develop and deploy cyber weaponry if the consequences are not understood by both military and civilian planners. While it is difficult to estimate the true potential for a catastrophic attack to spill over to kinetic warfare between states, the notion that the threat exists at all is cause enough to begin constructing a regime or legal framework through which to conduct cyber warfare.

History presents another lesson in that even with the best intentions and resources, a global cyber security regime will not transpire in short order. It will take many years to form an effective international consensus that might translate into a revision of the Law of Armed Conflict as spelled out by the Geneva Conventions. The operative concept is *regime.* And, the time to establish a global cyber security regime is *now*. As a proper follow-up to the innovative inaugural Tallinn CCD COE conference of 2009, NATO can and should play an important role by bringing together in short order the relevant stakeholders to outline a viable cyber security regime. Lt. Col. Walker quoted in the introductory epigraph to this paper, eight years ago properly challenge the legal community, and this writer has chosen to extend his challenges to the wider global policy community.

## References

[1] Walker, Jeffrey K. (2001) ‘The demise of the nation-state, the dawn of new paradigm warfare, and a future for the profession of arms’ *Air Force Law Review* (51:2001).

[2] Stars and Stripes (2009) ‘Pentagon Steps Up to Fight Cyber War’ (30 May 2009) http://www.military.com/news/article/pentagon-steps-up-to-fight-cyber-war.html?col=1186032310810

[3] Schogol, Jeff (2009) ‘Official: No options ‘off the table’ for U.S. response to cyber attacks**’**, *Stars and Stripes (*Mideast edition, 08 May 2009). http://www.stripes.com/article.asp?section=104&article=62555

[4] Gertz, Bill (2009) ‘Cyber warfare plans’ *Inside the Ring* (04 June 2009) http://www.gertzfile.com/gertsfile/InsidetheRing.html

[5] Reynolds, Jeffrey. (2005) ‘Collateral Damage on the 21st Century Battlefield’, Air Force Law Review (56:2005).

[6] Stephens, Dale and Michael Lewis (2005) ‘The law of armed conflict—a contemporary critique’ *Melbourne Journal of International Law* (6:2005).

[7] ‘Geneva Conventions: A Reference Guide’ (2009) Society of Professional Journalists. http://genevaconventions.org (Accessed: 01 June 2009)

[8] ICRC-International Committee of the Red Cross (2009) ’The mission’. http://www.icrc.org/HOME.NSF/

[9] Owens, William (2001) *Lifting the Fog of War* (New York: Farrar, Straus & Giroux).

[10] Libicki, Martin (1995) ‘What is information warfare?’ *ACIS Paper 3*: August 1995; National Defense University Press. http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html

[11] Hanseman, Capt. Robert G. (1997) ‘The realities and legalities of information warfare’ *Air Force Law Review* (42:1997)

[12] Schmitt, Michael N. (2003) ‘The sixteenth Waldmar A. Solf lecture in international law’ *Military Law Review* (176:2003).

[13] Keizer, Gregg (2006) ‘British Museum unveils WWII computer replica’ *InformationWeek* (08 September 2006). http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=192700296

*[14]* Antolin-Jenkins, Cdr.Vida M. (2005) ‘Defining the parameters of cyberwar operations: Looking for law in all the wrong places?’ *Naval Law Review* (51:2005).

[15] Tennant, Don (2009) ‘The fog of cyber war’ *Computerworld*, 27 April 2009.

[16] Kelsey, Jeffrey T.G. (2008) ‘Hacking into international humanitarian law: The prince-les of distinction and neutrality in the age of cyber warfare’ *Michigan Law Review* (106:2008)

[17] Aust, Anthony (2005) *Handbook of International Law* (Cambridge: Cambridge University Press).

[18] Marks, Paul (2009) ‘Pentagon readies its cyberwar defences’ *New Scientist* (16 arch 2009).

[19] Ki-moon, Ban (2009) ‘Secretary-General's remarks to the Advisory Board on Disarmament Matter’ (New York: 18 February 2009). http://www.un.org/apps/sg/sgstats.asp?nid=3717 http://www.un.org/apps/dsg/sgstatsarchive.asp

[20] ITU-International Telecommunications Union (2008) ‘ITU’s global cybersecurity agenda housed in Malaysia**’** (04 September 2008). http://www.itu.int/newsroom/press_releases/2008/27.html

[21] ITU-International Telecommunications Union (2009) 'ITU's global cybersecurity agenda housed in new centre in Malaysia: IMPACT headquarters in cyberjaya to focus on strengthening network security' (20 March 2009). http://www.itu.int/newsroom/press_releases/2009/08.html

[22] Knecht, Ronald and Ronald Grove (2001) *The Information Warfare Challenges of a National Information Infrastructure'*
http://web.archive.og/web/2001110717440/http://invorwar.com/mil_c4i//iwchall.hyml-ssim