Towards a Militarization of Cyberspace?

Cyberwar as an Issue of International Law

The rationale behind this study is that while cyberwar is gaining recognition as a “fifth battlefield”, policy makers and the general public have insufficient knowledge about the legal and strategic implications of this development. The project explores questions of relevance for policy and public debate, such as: How can policy makers develop legal mechanisms and procedures that allow for cybersecurity threats to be properly assessed? In creating a legal regime for Cyberwarfare, what dilemmas arise? Which legal considerations and constraints should shape the development of civilian and military cybersecurity institutions? Why is a critical perspective on the cyberwar discourse important for policy making? To address these questions, the project will undertake five thematic investigations:

1. Cyberwar as an issue of international law
2. Cyberwar in the NATO Strategic Concept: Some Issues
3. Distribution of Competence between Civilian and Military Authorities
4. The Relationship between International and National Institutions
5. The State, the Market and the Role of Public/Private Partnerships in Cyberwarfare

This working paper will discuss cyberwar as an issue of international law. The working paper examines some of the legal and strategic challenges that arise with respect to the development of effective international and national strategies to prevent, regulate and resolve cyberwar.
Towards a Militarization of Cyberspace?

Cyberwar as an Issue of International Law

Kristin Bergtora Sandvik          Peace Research Institute Oslo
Towards a Militarization of Cyberspace?
Towards a Militarization of Cyberspace?

Contents

About the Project .......................................................... 5
Executive Summary ......................................................... 7

Introduction ...................................................................... 11

Part I: The Role of Law in Constituting Cyberwar ............ 13

1. The Empirical Context: Situating the Quest for Legal Regulation in Contemporary Trends ............................................................... 15
   1.1. Critical information infrastructure (CII) as a matter of national security  15
   1.2. The globalization of information technology: citizenship and governance  15
   1.3. The rise of cyber threats: what, where and who ................................ 16

2. Situating the Quest for Regulation in the Institutionalization of Cyberwar 19
   2.1. The militarization of cyberspace ......................................... 19
   2.2. The cyber military-Industrial complex ............................. 19
   2.3. The internationalization of cybersecurity Issues ................ 20

3. Situating the Quest for Legal Regulation in Cybersecurity Discourse ___ 23
   3.1. Legalization as element of threat framing ............................ 23
   3.2. The place of law in popular cyberwar discourses ................ 24
   Summary ........................................................................ 25

Part II: Cyberwar - The Inside View ................................ 27

4. The Evolution of Cyberwar Discourse ............................ 29

5. Current Approaches ..................................................... 31
   5.1. Defining elements of cyberwar ........................................ 31
   5.2. Legal models ................................................................ 31
   5.3. Alternatives: the comprehensive legal approach ............... 33
   Summary ........................................................................ 34

Part III: Computer Network Attacks and the Jus ad Bellum .... 37

6. The Use of Force ........................................................... 39
   6.1. When does a CNA represent a prohibited use of force under the UN Charter? 39
   6.2. Chapter VII security scheme ........................................ 41
   6.3. What remedies are available to attacked states? .................. 41
   6.4. The content of self-defense ........................................... 42
   6.5. Attribution and state responsibility .................................. 42
   Summary ........................................................................ 43
Part IV: Computer Network Attacks and the Jus in Bello _________ 45

7. Targeting ____________________________________________ 47
  7.1. The basic distinction: protected and legitimate targets ________ 47
  7.2. Who can be attacked? ________________________________ 47
  7.3. Which objects can be attacked? ________________________ 49
  7.4. The prohibition on indiscriminate attacks ______________ 50
  7.5. Deceit and deception in cyber-attacks: the prohibition of perfidy 52
  7.6. Neutrality _________________________________________ 52

Summary ________________________________________________ 53

Conclusion ______________________________________________ 56
About the Project

This working paper is funded by the Norwegian Ministry of Defense as part of a three-year post doc entitled “Regulating Cyberwar: Understanding Challenges to Norwegian Security and International Law”, aimed at surveying the multidimensional nature of cyberwar. The rationale behind the study is that while cyberwar is gaining recognition as a “fifth battlefield”, policy makers and the general public have insufficient knowledge about the legal and strategic implications of this development. The project explores questions of relevance for policy and public debate, such as: How can policy makers develop legal mechanisms and procedures that allow for cybersecurity threats to be properly assessed? In creating a legal regime for Cyberwarfare, what dilemmas arise? Which legal considerations and constraints should shape the development of civilian and military cybersecurity institutions? Why is a critical perspective on the cyberwar discourse important for policy making? To address these questions, the project will undertake five thematic investigations:

(1) Cyberwar as an issue of international law
(2) Cyberwar in the NATO Strategic Concept: Some Issues
(3) Distribution of Competence between Civilian and Military Authorities
(4) The Relationship between International and National Institutions
(5) The State, the Market and the Role of Public/Private Partnerships in Cyberwarfare

This working paper will discuss cyberwar as an issue of international law. The working paper examines some of the legal and strategic challenges that arise with respect to the development of effective international and national strategies to prevent, regulate and resolve cyberwar.
Towards a Militarization of Cyberspace?
Executive Summary

Introduction
In recent years, cyber-attacks have been recognized as vital threats to national security, potentially amounting to acts of war. What are the implications? This working paper probes this issue by exploring the role of international law in providing a framework for governing cyber-attacks as threats to national and international security. The working paper aims to achieve two things: The first is descriptive, namely to offer a comprehensive and critical introduction to the legally relevant aspects of the cyberwar discourse. While exercises of legal line drawing are important and useful, they are also strategic and political. At the same time, many of the challenges pertaining to the understanding and conduct of cyberwar are not primarily of legal nature. The second objective has a normative rationale, namely to unpack the role of law in the current push by military, political and commercial actors to shift cybersecurity issues into the domain of warfare. The working paper considers that this development contributes to creating greater government and military control over civilian networks, leading to potential infringements on civil liberties.

Part I: The Role of Law in Constituting Cyberwar

Section 1 examines the rise of cyberwar on the international agenda and the attendant quest for legal regulation by pointing to three important contemporary trends: Critical information infrastructure (CII), such as the world wide web, and SCADA systems, have become key to critical infrastructure (CI), that is, those assets deemed central to the functioning of economy, society and national security. As information technology hardware and software have become more technically advanced, affordable and ingrained in daily life across the globe, a new digital landscape of citizen’s activism and governance practices have emerged. With democratic and undemocratic governments and commercial actors seeking increasing control over cyberspace, commentators express concern that this will mean the “end” of the internet by stifling freedom of expression as well as innovation. Finally, as the rate and severity of cyber-attacks continue to grow exponentially, with international organizations, governments and corporations being attacked on a global scale, the sense of urgency has increased dramatically at the policy level across the Western world.

Section 2 proposes that the institutionalization of cyberwar in itself generates a need for more law: In response to the notion of threat, a high number of countries have produced national security strategies over the past two years. A number of countries have also announced that they have, or plan to acquire, military cyberwar units. In reaction to these developments but also as a result of lobbying efforts, a new cybersecurity-industrial complex is emerging. In addition, cybersecurity issues are being internationalized. Partly intertwined with longstanding debates about internet governance, two streams of norm-developing efforts can be discerned at the UN level: an economic stream focusing on cybercrime and a politico-military stream focusing on cyber-warfare. Debates are dominated by intrastate disagreements as to how cyber-attacks should be categorized.
(particularly between the U.S and Russia), disagreements which also reflect part of the broader struggle for the control of the internet.

**Section 3** situates the quest for legal regulation in cybersecurity discourse. Cyberwar is frequently used as a metaphorical concept and the imprecise terminology for describing cyber-conflict often leads to hyperbole. Because words have meaning, and metaphors matter, attention must be paid to the role of law in sustaining them. Legal discourse functions as a way of constituting cyber-attack as threats to national and international security. The debate on cyberwar is dominated by three discursive approaches. The “cyber doom” argument actively calls for more national and international regulation, particularly the law of armed conflict, as a way of legitimating its own position. The skeptical position rejects the whole discourse on cyberwar, and hence also the call for bringing in the law of armed conflict. The pragmatist position partially accepts the framing of certain cyber events as threats to national and international security, but calls for a comprehensive legal approach, where the law of armed conflict is part of the framework.

**Part II: Cyberwar- The inside View**

**Section 4** explores policy initiatives and academic discussions that take cyberwar as a given political and technical problem for which law provides part of the solution. According to the inside view laid out in this section, “cyberwar” requires attacks on a sovereign state by another state or a sufficiently consolidated non-state entity. In essence, cyberwar involves the penetration of foreign networks for purpose of disrupting, dismantling, destroying or manipulating those networks, in order to achieve a strategic, military or economic advantage. The evolution of the cyberwar discourse can be traced from its inception as one of several forms of information war in the early 1990s, strongly connected to the thinking on revolution in military affairs (RMA), to its current status as a distinct form of warfare in need of legal regulation. The disagreement between those arguing for a new cyber-specific regime in international law and those considering existing norms sufficient began to emerge in the mid-1990s. Briefly superseded by discussions on cyberterror in the aftermath of 9/11, the discourse on cyberwar testifies to an ongoing militarization of cyberspace and cybersecurity issues.

**Section 5** prods the conceptual and definitional challenges that characterize the current debate. Which elements should go into a definition of cyberwar? A cyber-attack can result in damage or disruption in the virtual world and/or in the kinetic world. Whether a computer network attack constitutes a weapon of war depends on the scale, target, objective and outcome of the attack. At the same time, the availability of legal remedies hinges on the ability to identify who is behind the attack, what their intention is, what damage is incurred and whether causality between the attack and its consequences can be established. The legal debate is dominated by three positions on how the international community should regulate cyberwar. The first perspective sees cyberwar as difficult- or impossible- to regulate at the international level. The second position calls for new legal instruments while the third position mainly sees cyberwar as a problem of applying the law of armed conflict. The law of armed conflict model is currently being consolidated by way of a Manual on International Law Applicable to Cyber Warfare expected to be finalized in late 2012. An alternative model which indirectly challenges the concern with “war” as
the focal point of cybersecurity discourse, and proposes a “comprehensive” legal approach capable of addressing the full spectrum of cybersecurity issues is currently emerging.

Part III: Computer Network Attacks and the Jus ad Bellum

Section 6 surveys the key the lege lata (law as it exists) discussions in the jus ad bellum (law on the use of force) concerning the regulation of cyberwar. Central to the discussion is the use of force under the Charter of the United Nations. While commentators have mostly agreed that a cyber-attack may represent a prohibited use of force under art. 2 (4), the threshold levels for when a cyber-attack constitutes a use of force or an armed attack are still contested. Legal commentators also disagree on when a state may engage in self-defense under art. 51 in response to cyber-attacks; as well as on the specific requirements for attributing responsibility for an attack to a particular nation state.

Not unique to the case of cyberwar, the interpretation of the norms of the jus ad bellum is generally characterized by the different strategic logics and unequal power relationships between nations. Whether political actors support strict or permissive interpretations, will also depend on whether their field of responsibility is in the domain of military capabilities or in the protection of civilian infrastructure. National approaches to the use of force in cyberspace largely reflect those strategic positions generally taken on the use of force and the permissibility of self-defense in response to armed attacks.

From a doctrinal perspective, many questions remain unresolved: can the existing framework meaningfully differentiate between legal activities, such as cyber espionage, and illegal computer network attacks? What is the likelihood of reaching international consensus on the interpretation and enforcement in this area, when various types of states are likely to view cyber-threats differently and to distinguish differently between what counts as offensive and defensive measures? Will some states prefer legal ambiguity?

Part IV: Computer Network Attacks and the Jus in Bello

Sections 8 and 9 survey the key the lege lata (law as it exists) discussions in the jus in bello (law of war) concerning the regulation of cyberwar. The regulations applicable to cyberwarfare are mainly found in the Additional Protocol I relating to the protection of victims of international armed conflicts from 1977 (Part V on the civilian population), and in the law of neutrality as codified in the 1907 Hague Convention. Although interpretive disagreements remain, there is general agreement among scholarly commentators as to the applicability of these norms to computer network attacks. The interpretive focus is on making distinctions between the military and civilian sphere: Who is or isn’t protected from cyber-attacks and how does a transition between the two categories happen? Who can lawfully participate in hostilities? What is or isn’t protected from cyber-attacks and how does a transition between the two categories happen? To which means and methods must cyber-attacks conform to be legal? What are the rules concerning deceit and deception applicable to cyber-attacks? What respect is owed to neutral states, and what must states do remain neutral?
Towards a Militarization of Cyberspace?

The arguments about the thresholds for legality go to the heart of the ethics of war: While some commentators argue that a resort to cyberwar will mean more frequent targeting of civilians, others contend that rather than prevent the development of cyberweapons, the law of war should evolve to encourage states to use cyberweapons in some circumstances while also properly restraining their use in others. More broadly, the challenge for lawyers and force planners is to identify and conduct realistic exercises where relevant scenarios arise. In practice, a plethora of overlapping and competing legal regimes require states to adjust any offensive cyber-attack strategy to satisfy their obligations under various specialized regimes of international law, and to negotiate the relationship between international law obligations and domestic legal norms. However, a general problem in adapting law of war for cyberwar is that lawyers lack scientific and technical skills to analyze technological developments. Moreover, research on cyberwar is classified and thus inaccessible.

Conclusion
The working paper concludes by pointing to three observations: First, the focus on cyberwar as threat to national security and international peace may misspecify the solutions to cybersecurity issues: While international law offers a regulatory framework for a crucial but small part of the cybersecurity challenge, inadequate protection of critical information infrastructure and unsatisfactory coordination of domestic legal regimes remain insufficiently addressed by policymakers in most jurisdictions. The comprehensive legal approach offers a promising way forward. Second, the militarization of cyberspace calls for a concerted effort to promote a “cyber peace” agenda. How can policy makers ensure that sufficient attention is given to how international norm-making can be part of the work to ensure “cyber-peace”? Cyber peace could be promoted by delinking cybersecurity issues from armed force and by imposing a high legal threshold for treating them as equivalent. At the same time, cyber peace should not be defined only in the negative: attention must be given to the role of international law in the development of a substantive cyber peace agenda.
Introduction

The concept of cybersecurity is the site of constant renegotiation between the domains of the market and the state, and the civil and the military. An attacker can utilize numerous computer vulnerabilities that penetrate, interfere, disrupt, disable, steal, or destroy communications, vital information, and operating systems on numerous computer systems and networks.\(^1\) Methods of attack include \textit{malware} containing software such as \textit{viruses}, \textit{worms}, \textit{logic bombs}, and \textit{rootkits}; \textit{zero-day threats} that try to exploit software vulnerabilities; the use of DDoS, distributed denial of service attacks, frequently through the use of botnets (short for “robot networks”); or compromising computer security through human manipulation, so-called “social engineering”. These threats to cybersecurity are commonly classified as either lower level individual crime; organized crime; cyber espionage; cyber-terror; or as state-sponsored cyber-attacks.\(^2\) Significantly, such attacks often occur in the “twilight between criminal acts and acts of war”\(^3\), and boundaries may be blurred between black hat hackers, “patriotic hackers” and direct state participation.

The overarching issue addressed by this working paper is the following: Cyberwar, then known by its early moniker “information war”, or simply IW, has been on the radar of policy makers, security experts and military commanders since the inception of the Advance Research Projects Agency Network (ARPANET), the precursor to internet funded by the Defense Advanced Research Project Agency (DARPA) of the US department of defense, in the 1960s. However, only in recent years have certain types of cyber-attacks been recognized as vital threats to national security, potentially amounting to acts of war. What are the implications? This working paper probes this issue by exploring the role of international law in providing a framework for governing cyber-attacks as threats to national and international security. Focus is directed both at the labeling-process through which cybersecurity becomes an issue of “war”, and the ways in which law and ideas about legality operate inside cyberwar discourse.

The working paper aims to achieve two things: The first is descriptive, namely to offer a comprehensive and critical introduction to the legally relevant aspects of the cyberwar discourse. While exercises of legal line drawing are important and useful, they are also strategic and political. At the same time, many of the challenges pertaining to the understanding and conduct of cyberwar are not primarily of legal nature. The second objective has a normative rationale, namely to unpack the role of law in the current push by military, political and commercial actors to shift cybersecurity issues into the domain of warfare. The working paper considers that this development contributes to creating greater government and military control over civilian networks, leading to potential infringements on civil liberties.

There is no lack of law: Today, cybersecurity issues are governed by a plethora of national and international legal regimes, including computer law; criminal law; security law; human rights, the law of armed conflict- and an increasingly thickening international framework of cyber-specific norms. Yet, we have a very imprecise lexicon for describing

---


Towards a Militarization of Cyberspace?

cyberconflict⁴: In the context of international law, there is no agreed-upon definition of cyberwar, and there is deep disagreement about which attacks might amount to a cyberwar: how it starts, how it ends or how it should be conducted, as well as the potential legal ramifications.⁵ At the political level, whether an attack is classified as an economic or political-military issue by the government and the military will depend on the scale, sophistication and motivation of the attack, but also on the geopolitical and strategic resources of the country under attack, and the (attributed) identity of the attacker. With a burgeoning cyber-lobby, there is increasingly also a commercial logic to the classification of cyber-attacks as cyberwar. An international law for cyberwar will concomitantly be shaped by and shape these strategic and political considerations.

Most of the current writing on the legal regulation of cyberwar focuses either on the U.S military response or the interpretation and application of the norms of the Law of war. Much of this literature is scenario-based, relying on examples constructed either from available data or generic future scenarios. The working paper takes a skeptical approach to the current use of “factual” scenarios, noting that such “facts” (as well as legal arguments and references to specific bodies of law) are deployed to promote the ongoing militarization of cyberspace.

The working paper proposes that to provide knowledge about the role of law in governing cyberwar, it is important to unpack the mutually constitutive relationship between law, empirical developments on the ground and “the cyberwar discourse”. The working paper aims to develop a mapping of how cyberwar has evolved as a concept, including the role of law in constituting cyber-attacks as security threats, ultimately reaching a scale and impact where they are construed as acts of war. Why is there a quest for international regulation and how has it changed over time? What legal models have been proposed? To answer these questions, the working paper surveys relevant legal frameworks, policy documents and statements, academic literature, news coverage, conference material and social media sources.

---

⁵NATO, 2009, NATO and Cyber Defence Rapporteur Sverre Myrli, 027 DSCFC 09 E.
Part I: The Role of Law in Constituting Cyberwar
Towards a Militarization of Cyberspace?
1. The Empirical Context: Situating the Quest for Legal Regulation in Contemporary Trends

1.1. Critical information infrastructure (CII) as a matter of national security

In addition to the World Wide Web, cyberspace includes all networked digital activities, such as separate military defense networks, private sector networks and academic networks, as well as SCADA (supervisory control and data acquisition) systems. Together, these networks constitute society’s critical information infrastructure (CII), considered vital to the critical infrastructure (CI), which are those assets deemed central to the functioning of economy, society and national security. Key sectors of modern society rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. CII systems are in general regarded as inherently insecure. Most of the components are developed in the private sector, where profit motifs and competition, not security, drives system design: hence, a further explosion of computer and network vulnerabilities should be expected. At the same time, CII systems are seen as vulnerable because they constitute attractive targets.

1.2. The globalization of information technology: citizenship and governance

Since the late 1990s, information technology has become accessible across the globe. The long-held notion that the “virtual” world is a different “social space” than the “real world” is finally giving way to the understanding that there is one social world which contains both traditional and technologically advanced modes of communication and sites of social activity. This development has accelerated with the rise of social media over the past five years: The humanization of technology coupled with the increasing human dependence on technology is profoundly changing concepts of identity and citizenship, as well as the ways in which we are governed or accept to be governed. According to commentators, this global interconnectivity leads to “ill-understood behavior of systems, as well as barely understood vulnerabilities”.

In the 1990s, the relatively unregulated World Wide Web was commonly portrayed as an endless and chaotic highway without traffic rules, and thinking about how cyberspace would change governance was in its infancy. Today, the use of information technology is recognized as political practice: Wikileaks, the Arab Spring bloggers and the activities of the hacker group “Anonymous” are examples of citizen’s strategies to disrupt
power. At the same time, internet is no longer “lawless” or “without borders”. In fact, law is a key tool of governance: authoritarian and democratic governments have moved rapidly to obtain tighter regulation and more advanced technological means for control over the internet; and the filtering, denial (the so-called “kill switch”) and control of access is becoming widespread as a governance practice. Alternative, “bordered” internets that have emerged through national changes of the Internet’s architecture following national laws, technological developments enabling the implementation of certain policies. This has gradually led to a rejection of the “commons” notion and the extension of sovereign state control into cyberspace, according to experts affecting “architecture of the internet, its rules and governance, and most importantly, the values that shape cyberspace”. As governments and commercial providers intensify their quest for a “reform” of the internet, that will ensure greater political and commercial control, commentators express concern that this will mean the “end of internet” because control and excessive regulation will stifle innovation.

1.3. The rise of cyber threats: what, where and who

The rate, severity and targeting-range of cyber-attacks continue to increase exponentially. The four widely available hacking techniques deemed to produce most of the global “cyber-insecurity” problem include malware, client-server platform attacks, DDoS attacks and social engineering by humans. Malware contains software such as viruses, pieces of code designed to corrupt or destroy data, worms, self-replicating programs, logic bombs, programs designed to be triggered when specific circumstances are met, and rootkits. The latter can in turn contain Trojan horses, camouflaged programs that appear to be harmless, and backdoor utilities, usually tied to programs that have been Trojaned, securing backdoor entry to a secured network. A logic bomb is a piece of code inserted into a software system that will set of a malicious function when specific events occur or at a predetermined time. The second category is “client-Server Platform Attacks” designed to exploit Windows operating system vulnerabilities or Security Platforms Manipulation, by means of hacking into personal computer security software. A zero-day attack exploits computer application vulnerabilities that are unknown to the software developer. The third category is the most often-used form of infiltrating to enemy network infrastructure in the form of DDoS, or Distributed Denial of Service attacks. Using botnets as vehicles of attack DDoS attacks use botnets to overwhelm websites or serves with traffic, leading the target system to shut down. The fourth category is social engineering, which is shorthand for a number of practices including manipulation of others, illegal entry, stealing equipment or inserting infected memory sticks.

The range of victims of these attacks is broad, ranging from individual victims of harassment and identity theft to dissidents, human rights NGOs; corporations, international organizations, national governments and military installations. These attacks include spectacular events, like the Aurora attacks on Google, the Stuxnet attack at


the Natanz the uranium enrichment facility, the “war” over Wikileaks and more recently the hacking of Sony Playstation, and of Dutch authentication provider Diginotar. It also includes sustained targeting of international organizations, the oil and energy sector and defense contractors such as Vanguard Defense and Lockheed Martin.

Today, cyber-attacks, varying in severity and sophistication, are launched by many different groups for a range of motifs. In their assessments, security providers (based in the West) point out specific countries as havens for cyber insecurity: China, Brazil and United States are nearly always at the top of the list, but servers hosting attacks are distributed globally. However, the blurring of the virtual and the “real” coupled with the transnational character of these crimes, has created a shadowland with a completely new transnational topography: teenage computer geeks and computer experts at technology firms may also double as computer criminals, hactivists, spies or, increasingly, as cyber warriors on government sponsored brigades.


Towards a Militarization of Cyberspace?
2. Situating the Quest for Regulation in the Institutionalization of Cyberwar

2.1. The militarization of cyberspace
The Russian attacks on Estonia in the wake of the relocation of the Bronze Soldier of Tallinn (2007) and on Georgia (2008) together with the Stuxnet virus (2010) are considered “game-changers” in global cybersecurity. In most countries, attention to the practical national security aspect of cyberspace has until recently been uneven, despite considerable focus on the need to address cyber threats in national legal and policy documents. Over the last two years, however, there has been an increasing militarization of cyberspace, as more and more countries institutionalize cyberwar units and develop policies for offensive cyber capabilities.

The U.S. Cyber Command was inaugurated in May 2010 to integrate cyberdefense operations across the military. As a doctrinal matter, the Pentagon has made the strategic decision to proclaim cyberspace a “fifth domain” of warfare, on par with sea, air, land, and space. An U.S international strategy for cyberspace was launched in May 2011. The 2011 UK national security strategy made cyber-security a tier one priority, on par with international terrorism and major accidents. As of 2011, the UK is developing a cyber-weapons program. A number of other European countries released or updated their cyber strategies in 2010 and 2011, including France and Germany. Countries outside the Western hemisphere are also acquiring cyberwar capabilities: in July 2011, it became known that the People’s Liberation Army had unveiled its first department dedicated to tackling cyber war threats and protecting information security.

2.2. The cyber military-Industrial complex
Governments across the world are now increasing their spending on defensive and offensive cyber capabilities. While the US cyber military-industrial complex is unique, it is also indicative of a rise of such military-industrial complexes worldwide. Analysts have estimated the worldwide market to be as much as $140 billion a year. According to commentators, this complex can be compared to the military – industrial complex of the

---

cold war and may serve to not only supply cybersecurity solutions to the federal government, but to drum up demand for them as well. 27 The continued growth of transnational IT firms such as Symantec and MacAfee is in part fuelled by the spike in cyber-attacks, but also by the cyber threat assessments produced by these outfits, as potential opportunities for cybersecurity business present themselves in the public and the private sector. Commercial actors like Lockheed Martin, Boeing, L-3 Communications, SAIC, and BAE Systems have all launched cybersecurity divisions in recent years. Traditional defense contractors, such as Northrop Grumman, Raytheon, and ManTech International now invest heavily in information security products and services.

Commentators identify three types of arguments used by the proponents of this development: First, the widely cited arguments for more federal involvement in online security made by the Commission on Cybersecurity for the 44th Presidency (2008), which argued that “cybersecurity is now a major national security problem for the United States.” Second, the emergence of two groups of “cyber-security entrepreneurs”: Previously high profile members of US presidential administrations who now work in the private sector, include Mike McConnell, former National Security Agency chief and current Booz Allen Hamilton vice president and Richard A. Clarke, formerly special advisor to the president on cybersecurity and currently the chairman of Good Harbour Consulting. Together with Robert Knake, Clarke was also a co-author of the 2010 bestseller Cyber War: The Next Threat to National Security and What To Do About it.28 As supposed “experts” on the nature and origins of the Stuxnet virus, individual security specialists such as Ralph Langner29 and Eugene Kaspersky30 shot to international fame. The third is the “China syndrome”, which continues to gain traction: In reports and scholarly contributions, scenarios of future (but not too distant) cyberwars with China are featured prominently. Examples include Clarke (2010), Bronk (2011) and more recently by industry provider Northrop Grumman in a 2012 report prepared for the U.S.-China Economic and Security Review Commission.31

2.3. The internationalization of cybersecurity Issues

The international community is increasingly focused on institutionalizing the civil and military aspects of cybersecurity. In recent years, several efforts to agree on norms to regulate the threats posed in cyberspace have been made globally. At the same time, it is important to understand cybersecurity as an issue intimately intertwined with the struggle over internet governance and the long-standing disagreements between governments and the “quasi-governors” of the internet, such as the Internet Governance Forum, the Internet Engineering Task Force, and ICANN.32

---

28 Brito and Watkins 2011, id. above
30 See http://www.kaspersky.com/
32 For an overview, see Mueller, M 2010, Networks and States: The global politics of Internet governance, MIT Press; Mueller, M 2002, Ruling the Root: Internet Governance and the Taming of Cyberspace, MIT Press.
According to a recent working paper, while the UN Security Council does not mention the cyber aspect in its resolution on Georgia in 2008, and no resolutions were passed after the attacks on Estonia and Iran, the UN currently sees an “astonishing rate of norm emergence in cyber-space relative to typical international relations timelines.” Two principal streams of negotiations regarding cyber-security can be discerned: an economic stream focusing on cyber-crime and a politico-military stream focusing on cyber-warfare. For the economic stream, the central UN agencies are UNDOC (United Nations office on Drugs and Crime) and the ITU (the International Telecoms union). At the European level, ENISA (the European network and information security agency) was set up in 2004 to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to network and information security problems.

With respect to the politico-military stream, which is the focus of the working paper, a number of developments are notable: In response to the 2007 cyber-attacks on Estonia, NATO set up its Cooperative Cyber defense center of excellence in Tallinn. The Lisbon Summit Declaration of 20 November 2010 and NATO’s 2010 Strategic Concept emphasized cyber defense as a crucial aspect of the security of NATO, its member states, and its partner states. In 2010, for the first time, cybersecurity was brought into the NATOS strategic concept. NATO’s first official cyber defense policy was presented in June 2011.

At the UN level, cyberwar is tied up with the broader regulatory question of cybersecurity. Since the late 1990s, Russia has been particularly vocal in calling for a set of international rules, a call rejected by the U.S until very recently. This refusal has been explained as a rejection of Russia’s discursive shift from cybercrime to cyberwar: The U.S perception is that Russia will remain a haven for cyber-crime, but wants a cyber-treaty to compensate for national security cyber vulnerabilities.

In its International Strategy for Cybersecurity, the U.S pledges to work with “likeminded states” to develop shared norms for acceptable state behavior in cyberspace. Yet, in 2010, the U.S. reversed its long-standing policy position by co-sponsoring a draft resolution on cyber-security that has been introduced in the UN General Assembly by Russia since 1998.

Another (related) example of a clash of values is the reception of the international norm-making efforts of the Shanghai Cooperation Organization (SCO): The SCO is an intergovernmental mutual-security organization founded in 2001 by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. SCO has recently been strongly involved in cybersecurity issues. An SCO-accord adopted in 2009 defined “information war,” in part, as an effort by a state to undermine another’s “political, economic, and social systems.” The SCO proposed that the dissemination of information “harmful to the spiritual, moral and cultural spheres of other states” should be considered a “security

---


34 See http://www.ccccoe.org/


38 The strategy is available at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (last visited 13.03.2012).

39 Maurer, T 2011, id.
threat.” In 2011, the SCO proposed an international code of conduct for information security to the 66th UN General Assembly. The proposal, which included the principle that “policy authority for Internet-related public issues is the sovereign right of states”, was rejected.

40 Gjelten, T 2010, id.
3. Situating the Quest for Legal Regulation in Cybersecurity Discourse

3.1. Legalization as element of threat framing
This section gives attention to the role of law in framing cyberwar. As pertinently pointed out by cybersecurity expert Bruce Schneier “words have meaning, and metaphors matter...if we accept the military’s expansive cyberspace definition of "war," we feed our fears.” \(^{42}\) Does legalization, defined as the tendency to bring more and more aspects of international life into the ambit of law like processes\(^{43}\), in itself constitute a way of framing cyber-attacks as threats to national and international security? More specifically, is bringing the law of armed conflict into the discourse also constitutive of how we conceptualize cyber conflict? Threat framing is here taken to mean the process whereby particular agents develop specific interpretive schemas about what should be considered a threat or risk, how to respond to this threat, and who is responsible for it.\(^{44}\)

The 1990s saw a “rapid and considerable political impact of the widespread conceptualization of aspects of information technology as a security problem”\(^{45}\). Consecutively, cybercrime and espionage, cyber terror and cyberwar have been framed as existential threats to national security. Cybercrime started out as a very broad concept with various meanings, ranging from technology-enabled crimes to crimes committed against and for national security. Today, the codification of cybercrime in domestic jurisdictions as well as the widespread and transatlantic support for the 2001 European convention on cybercrime (into force in 2004) appear to have stabilized its content around a focus on criminal acts relating to the (mis)use of hardware and software, stealing and destruction of information for financial gain, to destroy competition or to gain a strategic advantage.\(^{46}\) Although cyber espionage is not prohibited by international law, it is usually criminalized at the domestic level. The lack of legislative attention to this issue is of course indicative of the reality that it while it is desirable to stop other actors from engaging in espionage, states would like to continue with their own espionage-practices.

By comparison, the cyber terror discourse has played out in the broader context of the global war on terror and its attendant culture of fear. However, as no international agreed definition of terror exists, talking about “cyber terror” has no defined focus, and as a result, in the absence of international events even broadly identified as “cyber terror” and in the context of the complicated international regulatory landscape, cyber terror has lost much of its traction as a national security threat.\(^{47}\)

\(^{46}\) Dunn Cavelty, M 2007 id; Tikk, E 2011 id.
\(^{47}\) For a broad overview of cyber crime legislation and current initiatives, see http://www.cybercrimelaw.net/Cybercrimelaw.html.
The working paper proposes that the current focus on cybersecurity issues as a mode of “war” governed by national security law and the law of armed conflict, can be understood partly as the outcome of a process of legal adaption whereby conceptions of threat emerge through circulation within and between supranational and domestic legal fields, and between legal and social fields.48 A key idea underpinning contemporary cyberwar discourse is the notion of national security as being under threat, due to inadequate infrastructure, funding, manpower, domestic policy and national and international legal frameworks. A perceived lack of legal regulation both of interstate conduct and of the obligation to provide cybersecurity by private companies, international organizations, and government bureaucracies is seen as creating vulnerabilities and constituting a threat to national security and to a peaceful world order.

Whether cyber war exists depends on the definition we give it, and will determine how governments may appropriately prepare and respond to various threats. Thus, it is necessary to understand the significance of using legal norms to describe cyberwar. Law is traditionally a means to institutionalize issues in global governance: over the last two decades, the world has been “witnessing a move towards law”.49 Seen this way, legalization also provides needed legitimacy for a process of militarization: While cyberwar scenarios in the literature frequently warn against the danger of “mass casualties”, such casualties have been notably absent in the two known cyberwars in Estonia and Georgia (where kinetic force produced casualties). Moreover, the dimension of territory which is so important for traditional legal definitions of war and battlefield is missing in cyberspace. Commentators have asked whether “warfare" is an adequate term for describing certain actions in cyber-space.50 In this context, the framing of cyberwar as a topic for LOAC and national security law is prognostic, it becomes about offering regulation of military solutions, and delineating the legal boundaries of the specific strategies, tactics, and objectives by which these solutions may be achieved.

3.2. The place of law in popular cyberwar discourses
A dominant feature of popular cyber discourse is the pervasiveness of what critical scholars have labeled “cyber-doom scenarios” or “cybergeddons”.51 Labels such as “digital pearl harbor”, cyber 9/11, “eWMDs” or “cyber-Katharina” are also used. Cyber-doom arguments are mostly propagated by “cyberhawks”, private sector security professionals with a past in security governance seeking contracts for delivering equipment and lucrative consultancies. American in its provenance but increasingly global in its reach, the cyber-doom imagery, echoing the cyber terror-discourse from a decade ago, conjures up scenarios where cyber-attacks on electric grids, dams and military infrastructure leads to disastrous environmental and societal consequences, including mass civilian casualties. These scenarios contain vivid descriptions of the catastrophic effects of collapses in air traffic, mass deaths at hospitals without power, nuclear reactors out of control and colliding trains. The 2010 bestseller by Clarke and Knake, Cyber War: The Next Threat to National Security and What to Do About it has been identified by more critical commentators as the archetypal harbinger of cyber-doom imagery.

50 Maurer, T. 2011 id.
In this type of imagery, Western countries and the NATO alliance are depicted as inadequately prepared for a looming cyberwar against Russia, China, North Korea and other adversaries. The cohort of external enemies has changed with geopolitical conjectures: In the late 1980s, the Soviets were the main information war adversary. From the mid-1990s, there has been a growing focus on China as the chief foe in a future cyber war. Calls for the application of the law of armed conflict- or more precisely- a new and cyber-specific LOAC instrument- is frequently voiced as part of the demand for tougher government action on adversaries, more comprehensive institutionalization of cyberwar in the national security infrastructure and more spending on both defensive and offensive cyber capabilities.

A second position rejects the militarization of cyberspace represented by the cyberdoom agenda. Critics argue that not only have the proponents of this agenda changed the story about who threatens what, how, and with what potential impact over time, but they have done so with very little evidence provided to support the claims being made. It is argued that there is no evidentiary basis that cyber warfare has ever been waged, or will be in the immediate future. This position argues that “cyber war” is not “war,” but in essence a computer security problem. A recent restatement of this position contends that cyberwar as a stand-alone act of war is simply not possible: in the paper "Cyber War Will Not Take Place" Dr Thomas Rid argues that hacking and computer viruses never actually kill people, hence cyber-attacks have not, and will not amount to stand-alone acts of war according to Clausewitz definition. Hence, the laws of warfare do not and should not apply.

A third position partially accepts the framing of certain cyber events as national security threats. It holds that regardless of labels, cyber threats are real and that various cyber tools and techniques are becoming increasingly important in international conflict. This position focuses on the necessity of protecting critical information infrastructure. According to this perspective, resilience is the best strategy to maintain national security and avoid escalation of international cyberconflicts. Resilience is achieved by using both humans and technologies to resist some attacks, absorb and mitigate others, and reach out to anticipate and stop other attacks. A comprehensive legal approach, including but not limited to the law of war, is an important component of the resilience toolbox.

Summary
This part has explored the role of law in constituting cyberwar as “war”, looking at empirical developments; the institutionalization of cyberwar; and cyber-security discourse. Three contemporary trends were seen as crucial for the current concern with cyber-attacks and their status as “war”. While critical information infrastructure has become essential to the economy, social life and national security, three new landscapes have emerged: The use of information technology and particularly social media is playing a key role in social change globally. At the same time, governments increasingly attempt to regulate and restrict access and content in cyberspace. The internet is no longer

---

54 Lawson, S 2011, id.
borderless and lawless. Finally, the rate and severity of cyber-attacks by hactivists and governmental entities continue to rise. As a result, cybersecurity issues are increasingly understood as issues of key political importance. The question is: what kind of political issue is cybersecurity?

The second subsection started from the assumption that the institutionalization of cyberwar generated a need for more law: the militarization of cyberspace amounts to de-facto recognition as cyberwar as “real war”, yet at the same time, it is represented as a new type of conflict fought by a new type of warriors very different from the traditional soldier type. This development is in part a result of the efforts of an emergent military-industrial cyber complex, which despite cuts in defense spending across the Western world experiences a financial bonanza,. The third tier in the institutionalization of cyberwar is the internationalization of cybersecurity and cyberwar at the global (the UN) and regional (NATO, OSCE, SCO) level. An interesting observation is that so far, discussions on cyberwar appear to be tied to the longstanding disagreement between Western governments and others, particularly Russia and China, as to how cyberspace should be governed.

The third subsection proposed that law and legal norms play a role in framing cyberwar as a threat to national and international security. It was argued that the so-called cyber doom argument, with lobbyists and the media as its chief proponents, sees law as an important tool in providing legitimacy for the claim that cyberwar is an existential threat: by calling on more law to engage an identified set of hostile powers, cyberwar acquires a more “settled” status.
Part II: Cyberwar - The Inside View
Towards a Militarization of Cyberspace?
4. The Evolution of Cyberwar Discourse

Recent years have seen a considerable militarization of the cybersecurity discourse, with cyberwar now frequently being described as a “war in the fifth domain”. Cyber-attacks can result in damage or disruption in virtual world and/or in the kinetic world. The push to define cyber-security in military terms, using metaphors of “war” and talking about cyberspace as a “battle domain” engenders a specific set of implications, with respect to the nature of cyber-attacks, the motivations of the attacker, the potential political ramifications of the attack and the appropriate means, including law, to prevent, defend and repeal such attacks. Consequently, the task of providing an adequate international legal framework for cyber-attacks has moved rapidly up the international political agenda. The conceptual and doctrinal link between information technology and warfare is not new, neither is the concern with defining cyberwar: As noted by Aldrich (1996), “how the law of war and international treaties proscribes the scope and use of information war hinges largely on how it is defined”.  

The early debates on information warfare were connected to the literatures on Revolution in military affairs, and the dawn of the information age. Attention was given to fleshing out more nuanced understandings of what the threat was, and what was “new” about war in an era of information technology. In their pioneering 1993 contribution, Arquilla and Ronfeldt offered a distinction between what they called “netwar”, by which they meant societal-level ideational conflicts waged in part through internetted modes of communication, and “cyberwar” at the military level.” The authors argued that while both netwar and cyberwar revolved around information and communications matters, at a deeper level they were forms of war about “knowledge”—about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries. In later seminal contribution, Libicki (1995) distinguished between seven different forms of information warfare, including command-and-control warfare; intelligence-based warfare; electronic warfare; psychological warfare; "hacker" warfare; economic information warfare; and cyberwarfare. Adding to the conceptual richness, Aldrich (1996) listed, in addition to information war, “info war”, informations operation”, “netwar”, “command and control counter war” (C2W), “third wave war”, “knowledge war” and “cyberwar.”

The initial debate on the need for an international response and the need to provide international legal regulation of information war emerged in the mid-1990s, as the empirical evidence of the possible impact of information war began to surface, and as computer crime and espionage became increasingly prevalent. Scholars focused on

---

62 Aldrich R.W 1996, id.
known information war techniques and the international legal implications of their use. While the scholarship on computer crime was already well established, considerable attention was given to the task of providing an analytical separation between information war, and cyber-crime and cyber-espionage.\textsuperscript{63}

Some early commentators argued that information warfare needed an international legal response, but that international law was geared towards an “antiquated” form of war, unable to keep up with technological developments.\textsuperscript{64} Others saw the existing international legal framework as adequate.\textsuperscript{65} Legal scholars gave extensive attention to more general treaty interpretation issues, the validity of article 2(4) as a norm in international law, and its applicability to cyber-attacks. In the latter part of the 1990s, the availability and affordability of information technology became more widespread, and the number of cyber-attacks more prevalent. Gradually, the legal analysis became more cyber-specific and the term “Cyberwar” began to replace information war (and other terms). At the same time, the division of labor between those advocating a new legal regime and those exploring existing normative structures continued. In the latter camp, the prescriptive emphasis was on the need for developing clearer rules for determining if and when cyber-attacks could be seen as an impermissible use of force.\textsuperscript{66}

In the aftermath of 9/11, the attention of legal scholars was re-directed towards the issue of “cyberterror”, before events in Estonia (2007) and Georgia (2009) saw a doctrinal return to the preoccupation with cyber-attacks as “war”.


\textsuperscript{65} Zengel, P 1996, \textit{Responding with Force to Information Warfare: Legal Perspectives}, Naval War College, Newport RI.

Towards a Militarization of Cyberspace?

5. Current Approaches

5.1. Defining elements of cyberwar
Two particular challenges arise in the attempt to define cyberwar. Providing a precise definition of cyberwar is linked to the challenge of defining cybersecurity in a sufficiently precise manner. Furthermore, it is necessary to link thinking about the conceptual vocabulary to thinking about the role cyber-attacks would play in actual conflict situations: much more likely than a “pure” cyberwar is the use of cyber-attacks as part of a military campaign.

While some experts have expressed skepticism to defining cyberwar in military terms, preferring instead a definition of cyberwar as “the use of information to attack information using information systems,” most proposed definitions focus on aggressive action by nation states or non-state actors. The most utilized definition is that of US DoD, (): Computer Network Attacks (CNA) are actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves. It has been observed it is unclear whether this definition covers operations that “manipulate computer information” or attacks aimed at causing damage extrinsic to the computer or computer network. The definition of CNA in the HPCR Manual on International Law Applicable to Air and Missile Warfare (1(m)) expands the definition to cover operations that “manipulate” computer information and aim “to gain control over the computer or computer network.”

Developing a precise conceptualization of when cyber-attacks become “war” requires a parallel vision of how cyber-technology can operate in war. In a useful contribution, Haussler (2011) delineates a four-point trajectory: first, the use of cyber technology can work as an enabler for traditional kinetic force used to launch a campaign. Second, the use of cyber technology may be one contributing factor in generating hybrid threats. Third, cyber capabilities may be used to degrade or deny decision-making and associated command and control capability, and/or achieve information superiority in the field of strategic communications, thus making a “significant contribution to campaign success”. Fourth, cyber capabilities can be used on their own.

5.2. Legal models
This section outlines the three positions on how the international community should regulate cyberwar that has so far dominated the legal debate. The first perspective sees cyberwar as difficult- or impossible- to regulate at the international level. The second position calls for new legal instruments while the third position mainly sees cyberwar as a problem of applying the law of armed conflict.

---


According to the first perspective, the inability of law to deal with the internet and information technology is often held up as a barrier against effective regulation, concerning the rapid development of technology and the cross-border nature of the internet.\textsuperscript{72} According to this perspective, cyber-attacks will often be too ambiguous, or too different from the categories of classic kinetic warfare to fall under the law of war framework.\textsuperscript{73} Furthermore, the regulatory task is extremely complex: an international framework for cyberwar must address the multidimensional nature of cyberwar, taking the strong civil/military, national/international and private/public dimensions into account. The difficult job of harmonizing cybersecurity norms at the national, bilateral and international level is further hampered by the clash of interest between governments and the private sector.\textsuperscript{74}

Moreover, an international agreement is difficult to achieve because the distribution of emerging cyber-capabilities and vulnerabilities is unlikely to correspond to the status quo distribution of power built on traditional measures including military and economic might.\textsuperscript{75} Even if a broad agreement could be reached, the challenges belonging to the well-known inventory of “regime choices” characteristic of such ventures persist. Stakeholders need to agree on who should make the new law, what form the rules should take, the role of institutions in overseeing the implementation and enforcement of the new law as well as the actual content and dynamism of the substantive norms.\textsuperscript{76}

The proponents of the second perspective, engage in an activity familiar to historians of military law: Faced with new military technology, legal scholars and practitioners habitually call for new legal instruments (currently, there is a vocal call for an international treaty to regulate unmanned combat aerial vehicles, UCAVs, better known as weaponized drones). As noted by a commentator, “the introduction of new means and methods of warfare has often been accompanied by the claim that technological developments are taking place in a legal vacuum and, consequently, demand a new legal paradigm”.\textsuperscript{77} Contemporary proponents of a new treaty hold that while cyberwarfare can be regulated by law, it represents a qualitative change in the meaning and nature of warfare, and a new international treaty regime dealing exclusively with cybersecurity and its status in international law should be developed. The scholars calling for a new treaty mostly focus on norms for jus in bello.\textsuperscript{78}

Briefly, borrowing Goldsmith’s model, these scholars believe that an important part of the solution to these challenges is an international treaty that does some or all of the following: (1) limits what states can do to one another in the cyber realm; (2) imposes on them duties to ensure that private actors within their borders do not engage in certain bad cyber acts; (3) establishes mechanisms of interstate cooperation to track and redress malicious cyber operations; (4) clarifies definitions (such as which acts constitute war and various crimes) in order to prevent mistaken interpretations and prevent misunderstanding or escalation; and (5) creates an international organization to facilitate

\textsuperscript{72}Tikk, E. 2011. id. p.100
\textsuperscript{73}Lewis, J.A. 2010. A Note on the Laws of War in Cyberspace, CSIS. available at
\textsuperscript{77}Haslam, E. 2000, Information Warfare, Technological Challenges and International Warfare, Oxford University Press, p. 158.
cooperation and monitoring (or a dispute referral mechanism, such as ICJ or the ICC). The new treaty-approach has been criticized for having “idealized a multilateral treaty akin to the Geneva Conventions”, which would neither be able to obtain sufficient state participation or be flexible enough to accommodate technological developments. Related propositions are to apply other legal instruments by analogy or the adoption of self-governing rules or non-legally binding norms (codes of conduct, rules of engagement) with the expectation that international legal rules will emerge from them in time.

The proponents of the third perspective appear to be the most numerous as scholars have now mostly arrived on a consensus that cyber-attacks may fall under the law of armed conflict and that the interpretation and application of the existing law of war framework is sufficient. Currently, this LOAC model is in the process of being consolidated. The Manual on International Law Applicable to Cyber Warfare is sponsored by NATO CCD COE and is produced by a group of “world-class international law and law of armed conflict experts”. The objective of this Manual is to develop authoritative reference on the international law applicable to cyber conflict. The manual is to be published in late 2012. It will be dived into “black letter rules “and accompanying “commentary”.

The manual will discuss the rights and obligations of states regarding cyber infrastructure and cyberspace, including sovereignty, jurisdiction and state responsibility, second, under jus ad bellum, the manual will discuss the use of force, Security Council action and self-defense. Under jus in bello, the manual will discuss a characterization of conflict, categories of persons, conduct of hostilities, specially protected persons and objects, deception and espionage, occupation, humanitarian assistance and command responsibility. A final section will deal with issues of neutrality, blockade and zones. The manual is modeled after the 1995 San Remo Manual on International Law Applicable to Armed Conflicts at Sea and the 2010 HPCR Manual on International Law Applicable to Air and Missile Warfare.

Like these manuals, the current project draws exclusively on European or American scholars. At the presentation of the manual at the 2011 NATO Coe conference in Tallinn, a participant from a “non-Western” country inquired about the composition of the expert group. How this will affect the legitimacy of the manual, particularly in competition with emergent initiatives from entities such as the Shanghai Cooperation Organization, is too early to say. Because the final version of the manual will be only after the completion of this working paper, the key debates under the law of armed conflict regime are presented in Part III and IV.

5.3. Alternatives: the comprehensive legal approach

In recent years, a fourth model emphasizing extensive coordination of legal approaches has emerged, namely the “the comprehensive security approach”. While this model integrates the cyberwar component, it considers a broader spectrum of threats to national and international security, as it links the danger of cyber conflict to cyber-threats to

81 Hollis D.B 2007 id., p.18.
83 Hollis D.B 2007 id.
critical infrastructure. This approach is based on the notion that the obstacles to a better cybersecurity are not technical, but policy based on outdated analysis. According to Eneken Tikk (2011), on whose work this section is based, the need for such an approach has been acknowledged on the international level only in the past few years, while national calls for a broad approach to cybersecurity date back almost a decade.

Under the «comprehensive approach”, law is seen as a required element for cybersecurity: while cybersecurity is not understood as a new domain, it is seen as a new strategic issue, posing new challenges and complex issues. In this context, the problem is identified as gaps in regulation and legal practice: the gaps in themselves create vulnerabilities. Moreover, it is emphasized that legal interpretation must be more cognizant of technology as well as its social use. Similarly, there is a need to clarify legal authority, and coordinate it between private stakeholders, national CERT-teams, law enforcement and the military: today’s fragmented mandates engender opportunities for malicious activity.

The need for a comprehensive approach derives both from architecture of internet and emerging cybersecurity threats and incidents. The architecture of the internet and the set-up of the information society mean that no country or organization can come up with an all-encompassing solution. The critical information structure on which government, military and information society rely, is mostly privately owned. These are systems with security standards developed in peace time and within a commercial frame. Emerging security challenges require management from a number of stakeholders – information technology experts, national policy makers, diplomats, military commanders and intelligence communities.

In short, what is needed is a substantive framework for addressing the full spectrum of cybersecurity: an approach combining considerations of threat, deterrence and response from different areas of authority and responsibility, thereby aiming at eliminating gaps between different aspects of cyber incident prevention, detection, response and recovery. Such an approach requires a systematic development, interpretation and application of legal areas and instruments in a number of legal fields, including information society and telecommunications, cybercrime, national security and armed conflict. This would involve expertise across legal, policy and technological boundaries. This might or might not entail the need for special regulation of cyberwarfare: a comprehensive approach will in any event be a necessary interim step for determining which aspects of cybersecurity would require additional international regulation.

Summary

In the mid-1990s, the term “cyberwar” began crystallizing in the literature and policy making circles as one of several forms of “information war”. The tension between positions arguing that cyberwar represents a new type of conflict in need of new legal norms, and conversely that the existing legal framework is adequate, has been present in the cyberwar discourse almost since the beginning. For a period overtaken by a “cyberterror” discourse in the years after 9/11, the concept “cyberwar” began to dominate the cybersecurity agenda after the Estonia attacks in 2007, and became an important topic on the general international agenda from 2010. In political and legal terms, the rise of cyberwar entails a considerable militarization of cyberspace that goes in tandem with a growing government-interest in controlling popular uses of the internet.

85 Lewis 2011, id.
In the literature, there are several competing approaches as to how cyberwar should be conceptualized and the legal models appropriate for governing it. The absence of a commonly agreed definition of cyberwar has been a problem for policy makers—too narrow and too broad definitions create challenges with respect to divisions of labor between civil and military domains, between the government and the private sector and between national governments and international entities. At the same time, it is vital that any theoretical notion of cyberwar is linked to an understanding of the role cyber-attacks may play in a conflict: There is a gliding scale from cyber-attacks as the enabler for kinetic force to cyber-attacks as armed attacks in their own right.

The legal debate on cyberwar has been dominated by three approaches: that cyberwar is difficult to regulate, that new legal instruments are needed or that the challenge lies in applying existing norms to cyberwar in a proper manner. The Manual on International Law Applicable to Cyber Warfare codifies the latter approach by attempting to provide a re-statement of how the law of armed conflict applies to cyberconflict.

An alternative approach indirectly challenges the concern with “war” as the focal point of cybersecurity discourse, and proposes a comprehensive legal approach capable of addressing the full spectrum of cybersecurity issues. This approach focuses on deploying a variety of legal instruments and to combine considerations of threat, deterrence and response from different areas of authority and responsibility.
Part III: Computer Network Attacks and the Jus ad Bellum
6. The Use of Force

6.1. When does a CNA represent a prohibited use of force under the UN Charter?

A law of force for cyberconflict must be capable of balancing territorial jurisdiction, sovereign responsibility, and the use of force. The higher the threshold for considering a cyber-attack to be a prohibited use of force, the higher the threshold at which cyber-attacks contribute to the escalation of a conflict. The starting point is that except in self-defense or when authorized by the UN Security Council, military attacks are illegal. According to article 2(4) of the UN Charter,

“All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

This provision prohibits a state from either threatening or using “force” against another state in the international community. Article 2(4) only prohibits the use of force; it does not authorize any response to a use or threat of force. Only two exceptions exist to this prohibition: actions authorized by the Security Council in response to “threats to peace” under article 39, and forceful acts of self-defense under article 51.

Since the drafting of the UN Charter, the reach of the term “force” has proven contentious. Article 2(4) has been described as “a complex operational code as to those coercive acts the international community, or at least the politically relevant members thereof, accept as lawful”. Three different views have been presented: One view of Article 2(4) focuses on the general effect of the article: that it prohibits coercion. Advocated at various times by the third world or the old Soviet bloc, this view has unsuccessfully pushed the notion that “force” includes other forms of pressure, including political and economic coercion threatening to independence. A second approach focuses on force as interference, specifically, the violation of states’ rights of sovereign dominion through acts such as propaganda or political subversion. The dominant view is based on the long-standing push to define force narrowly, as applying to military attacks or armed violence, and excluding economic and political coercion. Particularly the US and its major allies have advocated “bright lines” and resisted expansive interpretations and flexible standards.

According to the most restrictive legal view of cyber-attacks, they can categorically never constitute “force” in a way comparable to an “armed attack.” Some legal experts have demanded that to qualify as “force” a cyber-attack must produce “violent consequences.” Today, this restrictive view has largely been abandoned, and attention is directed towards determining when cyber-attacks fall below use of force, and when they are equivalent to a use of force that amounts to armed attack.

Graham’s model of analytical approaches is useful for distinguishing between interpretive frames:

---

87 Waxman, M.C 2011, id.
The “instrument-based approach” holds that the determination of whether or not the standard has been breached depends on the type of the coercive instrument—diplomatic, economic, or military—selected to attain the national objectives in question. A concrete assessment must be undertaken to determine whether the damage caused by a cyber-attack could previously have been achieved only by a kinetic attack.

The “strict liability approach” automatically deems any cyber-attack against critical national infrastructure to be an armed attack, based on the severe consequences that could result from any attack on such infrastructure systems. This broad view is based on an interpretation emphasizing the dependence of modern society on critical information infrastructure, suggesting that consequences of attacks waged through non-military means can often cause much more harm or pose greater threat than military ones.

The “effects-based approach” does not attempt to assess whether the damage resulting from a cyber-attack could previously have been achieved only through a kinetic use of force. Instead, the consideration is the overall effect of the cyber-attack on the victim state. However, this leaves us with the challenge of quantifying effects and establishing causal links: There will be “easy cases”, where CNA intended to directly cause injury, death or physical destruction can reasonably be characterized as an armed attack. Destroying the power grids of oil rights or hospitals would be typical examples. However, “hard cases” involving CNA which do not cause physical damage or injury, or do so indirectly, are difficult to classify, whether they concern temporary irreversible interference with computer system or introduction of malware with unknown future capacity for destruction.91

The much-cited Schmidt-model offers a framework for determining effects on a case-by-case analysis, considering both the qualitative and quantitative aspects of an operation, focusing on what historically made military force special in international law. In his model, Schmidt outlines six criteria: How severe is the attack with respect to threatening injury or destruction of property? How immediate are the negative consequences? How direct are the negative consequences and how invasive is the act causing the harm? What are the actual measureable effects and are the consequences presumably illegitimate, that is do they represent a prohibited application of violence? According to the Schmidt-model, the consequences of a cyber-attack should be measured against these criteria to consider whether they more closely approximate the consequences of the sort characterizing armed force or if they are better placed outside the use of force boundary. The model has been criticized for having logical flaws and for being difficult to operationalize.92

Finally, to constitute a prohibited use of force, who should the attack be directed against? In a traditional attack, whether the target is military or civilian does not make any different. The state where the target is located is entitled to self-defense due to violation of territorial integrity breach. Whether the computer network is run by corporation based in third state or computer system is located outside the target-states borders is not relevant. However, there is a requirement that the armed attack was carried out “with the specific intention of harming”. Hence where the attack lacked intention or was intended for a different state, the right to self-defense does not arise.93

6.2. Chapter VII security scheme

When a computer network attack is deemed to amount to a threat to peace, a breach of peace or an act of aggression, the Security Council may authorize a given set of responses. Article 39 grants the United Nations Security Council authority for responding to threats and acts of aggression:

“The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security”.

The standard allows the Security Council to authorize a response by force to any situation that might provoke a breach of the peace, based on a factual, not a juridical situation. However, Article 39 determinations and resultant use of force recommendations are difficult and time-consuming to achieve. Article 41 gives the Security Council authority to adopt measures “not involving the use of armed force,” and explicitly recognizes that such measures include the “complete or partial interruption of economic relations” or “communication”. Article 42 provides the Security Council with the authority to react forcefully pursuant to a CNA that amounted to a use of force under art. 2(4), i.e. to authorize member states to use force. While part of the international community’s toolbox to deal with cyber-attacks, neither provision appears to be very practical in the context of cyber-attacks as we know them today. This however, may change.

6.3. What remedies are available to attacked states?

By declaring that “Nothing in the Charter shall “impair the inherent right of individual or collective self-defense if an armed attack occurs” against a UN member” Article 51 carves out an exception to Article 2(4)’s prohibition on the use of force. However, the state’s right of self-defense is restricted to to situations involving armed attack, a narrower category of act than Article 2(4)’s use of force. Hence, action under article 39 does not trigger a right to act pursuant to article 51. Because “Armed attack” is not defined under international law, the concept cannot be limited to specific weapons. The higher the threshold for permitting armed self-defense under article 51, the lower is the likelihood of escalating a conflict.

Two analytical models have been put forward to facilitate the application of the “use of force” criterion. According to a narrow view, self-defense should be limited to operations which are de-facto armed attacks. The focus is on the consequences of attacks rather than on the object of the attack or on the intentions of the attacker.

According to a broad view, the threat of use of force demonstrates hostile intent and triggers a right to anticipatory self-defense. Depending on the target and if the intruders actions show hostile intent, the victim nation may consider such actions an armed attack. The lower the threshold for when a CNA constitutes a use of force or armed attack, the more flexibility in anticipatory self-defense. The requirement is that the state demonstrates sufficiently the imminence of the anticipated attack, a requirement that is difficult to meet with respect to cyber-attacks. The scope of anticipatory self-defense has been controversial in international law over the past decade. According to its advocates, the right to anticipatory self-defense to counter a cyber-attack arises if the CNA is part of an overall operation culminating in armed attack; if the CNA is an irrevocable step in an?

---

94 Graham, D. E 2010 id., p. 89.
imminent (near-term) and probably unavoidable attack; and finally, if the defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.  

The view that it is not the CNA that is actually being defended against, but the overall armed attack, is probably correct. Thus, compliance with the requirement that acts in self-defense be proportional is measured against the armed attack, not the CNA. For the same reason, the attack need not be against the facility that launched the CNA or even designed to counter this or other computer network attacks.

6.4. The content of self-defense

International law requires that appropriate self-defense must be necessary and proportional. A state meets the requirement of necessity when it becomes evident that, under the prevailing circumstances, the state cannot achieve a reasonable settlement of a dispute through peaceful means. “Proportionality” requires that state limit self-defense actions to the amount of force required to defeat an ongoing attack or to deter a future attack. The exercise of cyber self-defense can be conducted through passive (computer security, law enforcement) or active/offensive defenses. The latter is a much more controversial approach, and has until recently little discussed by government officials.

Active defenses involve electronic countermeasures that attack an aggressive computer system, immobilizing that system and thus halting the cyber-attack. Real-time disabling response consists of destroying the equipment used. An appropriate in-kind response, though legal, still raises questions: Can it be routed through third-countries, potentially violating their neutrality? How can it be guaranteed that erroneous targeting does not take place, i.e that correct attribution is being made? It is important to note that an active defense is not possible when the victim state lacks the technology to conduct it or when the aggressor does not have a sufficiently developed computer network to hit.

6.5. Attribution and state responsibility

It remains a technical challenge for forensics to link a CNA conclusively to the responsible party. This not only creates a problem of accountability after the attack, but the difficulty in identifying perpetrators also makes it difficult to employ deterrence as a strategy. Moreover, active defenses and deterrence may require differential confidence levels in how solid the attribution needs to be. The problem of attribution also affects the conversation in the international community about cyber-attacks and how to regulate them: it becomes problematic to go public about attacks, and to agree on attack-patterns.

The traditional criterion in international law is “conclusive attribution”, which poses difficulties in the context of cyberwar. In its place, a model of state responsibility for cyber-attacks based on “imputed” responsibility has been proposed. This applies to cyber-attacks conducted by a state’s own citizens, and to all non-state actors who launch such attacks from within a state’s territory. This includes civilian hackers as members of government agencies or parastatal entities like privatized corporations or independent contractors empowered by law to exercise some degree of governmental authority. The

---

95 Schmitt, M.N 1999, id; Roscini 2010:122.
96 Schmitt, M.N 1999, id.
98 Waxman, M.C 2011, id.
hackers could also be not *de jure* organs of a state but rather individuals or corporations hired by states in order to conduct cyber-attacks.

Such imputed state responsibility for cyber-attacks is premised on the existence of an affirmative duty of states to prevent their territories from being used as launching pads for such attacks. The state has the obligation to enact and enforce adequate criminal laws; to conduct meaningful, detailed investigations into cyber-attacks; to prosecute those who have engaged in these attacks and to cooperate with the victim states’ own investigations and prosecutions of those responsible for the attacks.\(^\text{100}\)

A state is in violation of its obligations if it becomes a sanctuary state for CNA. Traditionally, the standard for assessing state responsibility was referred to as the “effective/direct control test”. Because this is a very difficult standard to meet in the context of CNA, and would make self-defense difficult, commentators propose an “overall control standard”, where a state acquires responsibility for the actions of non-state groups using a state’s territory as a base of operations.\(^\text{101}\) A violation of this responsibility arises if it fails to comply with the obligations outline above. Conversely, some commentators argue that keeping the stricter “effective control” test will prevent states from being frivolously accused of being behind cyber-attacks.\(^\text{102}\)

**Summary**

Not unique to the case of cyberwar, the interpretation of the norms of the jus ad bellum is generally characterized by the different strategic logics and unequal power relationships between nations. Whether political actors support strict or permissive interpretations, will also depend on whether their field of responsibility is in the domain of military capabilities or in the protection of civilian infrastructure. National approaches to the use of force in cyberspace largely reflect those strategic positions generally taken on the use of force and the permissibility of self-defense in response to armed attacks. At the same time, it is possible to ask if the institutionalization of cyber armies in itself indicate a de-facto acceptance among states that cyber weapons are weapons systems with the potential for armed attack. The scholarly community has largely abandoned its erstwhile stance that CNA could not constitute a use of force or an armed attack.

From a doctrinal perspective, many questions remain unresolved: can the existing framework meaningfully differentiate between legal activities, such as cyber espionage, and illegal CNA? What is the likelihood of reaching international consensus on the interpretation and enforcement in this area, when various types of states are likely to view cyber-threats differently and to distinguish differently offensive attacks from defensive measures? Will some states prefer legal ambiguity? Traditionally, treating something as armed attacks triggering self-defense rights under article 51 has had deterrence value: as CNA capabilities proliferate, will a permissive authority to resort to armed force against cyber-attacks introduce greater security instability to the international system by undermining constraints on military responses to non-military harms?\(^\text{103}\)

---

\(^{100}\) Graham, D. E 2010 id., p.94.

\(^{101}\) Note also that according to the ILC draft articles (art.11) on state responsibility, conduct becomes attributable if a state endorses them post facto (Roscini, M. 2010, id. p.:101-102).

\(^{102}\) Roscini, M 2010, id. p.100.

\(^{103}\) Waxman, M.C 2011, id.
Part IV: Computer Network Attacks and the Jus in Bello
Towards a Militarization of Cyberspace?
7. Targeting

7.1. The basic distinction: protected and legitimate targets

The Jus in bello, or more narrowly “international humanitarian law” (IHL), is the “body of law concerned with what is permissible, or not, during hostilities, irrespective of the legality of the initial resort to force by the belligerents.”\(^{104}\) The conduct of cyberwar is primarily regulated by the Additional Protocol I relating to the protection of victims of international armed conflicts from 1977 Part V on the civilian population\(^{105}\) (hereinafter AP I) and the law of neutrality as codified in the 1907 Hague Convention.\(^{106}\)

Who is or isn’t protected from CNA attacks and how does a transition between the two categories happen? Who can lawfully participate in hostilities? The basic rule is AP I art. 48, which states that

“In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.”

The protection requirement renders a specific category of potential targets off-limits, while the distinction requirement extends protection to cases where civilians and civilian objects may not be directly targeted but where there is a high likelihood of striking them. The prohibition is on attacking non-military objectives through the use of violence, not on targeting them.

When should a CNA be considered a violent attack? According to AP I art. 49 (1), “‘Attacks’ means acts of violence against the adversary, whether in offence or in defence.” The literature indicates that the threshold for the determination of an attack is consequence-based: the relevant criterion is whether the attack generates violence equivalent to violence produced by kinetic force. Infliction of “human suffering” is required to cross the threshold. Disabling of an object, such as shutting down but not destroying the electricity grid qualifies as an attack, as long as it results in civilian death or injury. Conversely, inconvenience or financial loss caused by a CNA is not an “attack”.

7.2. Who can be attacked?

Who is or isn’t protected from CNA attacks and how does a transition between the two categories happen? Who can lawfully participate in hostilities? Civilians may not be the object of military attacks, and do not have a right to participate in hostilities. A civilian is everyone not considered a combatant. With respect to legal interpretation, doubts as to the character of an object or individual are to be resolved in favor of a finding of civilian status. Setting out a negative definition, AP I art. 50 states:

“A civilian is any person who does not belong to one of the categories of persons referred to in Article 4(A)(1), (2), (3), and (6) of the Third Convention and in Article 43 of this Protocol.”

---


\(^{105}\) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

\(^{106}\) Hague Convention of 1907 (v) The Rights and Duties of Neutral Powers and Persons in Case of War on Land
Towards a Militarization of Cyberspace?

According to AP I art. 51 (1), the “civilian population and individual civilians shall enjoy general protection against dangers arising from military operations”.

According to AP I art. 51(2) “The civilian population as such, as well as individual civilians shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.”

Conversely, combatants are by nature valid targets and may be directly attacked as long as the method and means used are consistent with IHL restrictions. AP I art. 43 (2) defines combatants as “[m]embers of the armed forces of a Party to a conflict”. Members of the armed forces have the right to participate directly in hostilities. The law of war indicates state affiliation as a precondition for combatant statutes, in addition to four enumerated criteria. AP I art. 43 (1) enumerates three criteria for “armed forces”: That they are (1) under a command responsible to a Party for the conduct of its subordinates, (2) that they are subject to an internal disciplinary system that enforces compliance with the rules of international law applicable in armed conflict. AP I art. 44 requires that combatants (3) “distinguish themselves from the civilian population” and (4) “carry[y] arms openly.”

Commentators have argued that in the case of cyber-attacks, the four enumerated combatant criteria provide unclear answers: In the absence of close combat, the requirement of distinction is less significant; As opposed to conventional attacks, where defenders respond to the combatant himself, CNA victims are more likely to respond to the means or method of attack. Furthermore, in terms of command responsibility, Cybercombatants are typically not isolated, and thus are unlikely to be forced to make autonomous discretionary decisions without the assistance of leadership and specialized staff. Finally, in CNAs the requirement that combatants be subject to an internal disciplinary system takes on reduced significance as well, as cybercombat could easily be conducted from domestic territory, where municipal criminal laws attach. It has been argued that focus should instead be given to the criterion of state affiliation.\(^\text{107}\)

A question of high practical significance is how a civilian may lose his or her protected status and become a legitimate target. The exception in AP I art. 51 (3) for civilians who “takes direct part in hostilities” is crucial for determining who is a legitimate target of a CNA. The individuals working on government cybersecurity issues, including maintenance of military assets or conduct of military operations, are increasingly private, civilian contractors. The different roles played by contractors in producing a host of different CNA effects pose legally complex questions about when an individual will become a legitimate target. Two interpretations of the “direct participation in hostilities” criteria have been advocated. A narrow interpretation includes only civilians whose work is to cause direct damage to or interfere with computer networks through CNA. According to a broad interpretation, “mission-essential” civilians working at a base during hostilities, also those not engaged directly in acts of war, should be viewed as legitimate targets.\(^\text{108}\) The legal consequence of being directly targetable is that injuries caused to such contractors would not be calculated when assessing whether an attack is proportional. A narrow interpretation of the “direct part in hostilities” standard preserves contractors protection as civilians. Civilians without state affiliation who directly engage in a computer


Towards a Militarization of Cyberspace?

7.3. Which objects can be attacked?
What is or isn’t protected from CNA attacks and how does a transition between the two categories happen? According to AP I art. 52 (1) “Civilian objects shall not be the object of attack or of reprisals”. Civilian objects are all objects which are not military objectives. AP I art.52(2) defines targetable military objectives as “those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”

It is thus necessary to establish the nexus between the object to be attacked and military operations: what constitutes “an effective contribution”, and what kind of contribution would offer a “definite advantage”? The growing interconnectivity between military and civilian critical information infrastructure makes this determination complex. According to a narrow interpretation supported by the ICRC, military objects are those “directly used by the armed forces” (e.g. weapons and equipment), locations of “special importance for military operations” (e.g. bridges), and objects intended for use or being used for military purposes. Conversely, the US embraces an expansive interpretation, including in the wording economic targets that “indirectly but effectively support and sustain the enemy’s war-fighting capability.”

Two exceptions are important, namely the prohibition on attacking those military objects that are either considered “dual use” or “indispensable”. A dual-use object is one that serves both civilian and military purposes. If an object is being used for military purposes, it is a military objective vulnerable to attack, including computer network attack, even if the military purposes are secondary to the civilian ones. An object that has the potential for military usage, but is currently used solely for civilian purposes, is a military objective if the likelihood of military use is reasonable and not remote in the context of the particular conflict under way. Under the category of “Specially protected objects” there is a prohibition of attack even if the objectives are also military objectives.

AP I art. 54(2) prohibits attacks that starve the civilian population or causes them to move away, by denying it “indispensable objects” for survival, even if enemy armed forces are the intended “victims” of the attack. Indispensable objects include such items as foodstuffs, crops, livestock or drinking water. Under this restriction, computer network attacks against, for instance, food storage and distribution system or a water treatment plant serving the civilian population is prohibited even if military forces also rely on them. AP I arts. 35(3) and 55 prohibit military operations likely to cause widespread, long-term and severe damage to the environment. AP I art. 56 prohibit an attack on dams, dykes and nuclear electrical generating stations, if the attack might “cause the release of dangerous forces [e.g. water or radioactivity] and consequent severe losses among the civilian population”. AP I art. 12 applies to civilian and military medical units, including hospitals. The requirement of the belligerents is here “to respect” medical facilities by not attacking or harming them, and not interfering with their work. This includes a prohibition on shutting down a hospital power grid as well as the corruption of patient

---

110 Schmitt, M 2002, id.
111 Schmitt, M 2002, id.
data base. The protected status ceases if the facility is used to commit, outside their humanitarian activities, acts harmful to the enemy.  

7.4. The prohibition on indiscriminate attacks

To which means and methods must CNA conform to be legal? The core prescriptions on striking legitimate targets are based on the principle of discrimination, which has three elements: The prohibition on indiscriminate attacks, the proportionality consideration and the obligation to take precautionary measures.

AP I art. 51(4) prohibits indiscriminate attacks. The discrimination requirement here is twofold. Applied to weapons, it prohibits the use of those that are incapable of distinguishing between combatants and military objectives on the one hand and civilians, civilian objects and other protected entities on the other. In general terms, IHL prohibits means and methods that cause superfluous injury or unnecessary suffering. As a result certain types of weapons are not allowed and the way other weapons are used is restricted. AP I art. 51(4)(b) and (c) define as indiscriminate those weapons “which employ a method or means of combat which cannot be directed at a specific military objective” or “those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.” A means of combat is defined in the Commentary on Additional Protocol I as a “weapon”, whereas a method of combat is the way in which a weapon is used. A CNA is part of a weapon system when it can cause injury, death, damage and destruction. Applied to tactics and the use of weapons, the discrimination criteria requires that an effort be made to distinguish between these two categories, civilian and military, when conducting military operations. Prohibiting indiscriminate use, AP I art. 51(4) (a) refers to “those which are not directed at a specific military objective”.

The principle of discrimination will play an important role in operations that carry high risk of civilian losses. Here, IHL requires military commanders to “know not just where to strike but be able to anticipate all the repercussions of an attack.” Opposite, humanitarian law will likely ban a cyber-attack that would be the “direct and intentional cause of [civilian] death and destruction.” However, for the spectrum in the middle, it is unclear how the principle of discrimination would act as guidance due to the highly interconnected nature of the military and civilian networks, which renders much of the Internet a dual-use target.

According to the second requirement, an attack is indiscriminate as violating the principle of proportionality when it “may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated”. Proportionality governs those situations in which harm to protected persons or objects is the foreseeable consequence of an attack, but not its intended purpose. To fulfill the criteria, the advantage must be “substantial and relatively close”, and calculated as the advantage to the overall operation, not the success of the individual attack. Force planners and decision-makers have a duty to ascertain likely damage or injury, with the assistance of adequate technical expertise. In the context of CNA, it is a particular challenge to

112 Dörmann, K. 2004, id.
address indirect and non-immediate effects owing to the interconnectivity between military and civilian systems, without the full knowledge of how these systems function and to what other systems they are linked. The proportionality principle may be violated due to insufficient understanding of the target for the attack; an inability to estimate the appropriate amount of force used, or the inability to ensure accurate targeting. 114

Finally, according to the third requirement, AP I art. 57 require the party to take “all feasible precautions” in the choice of means and methods of attack with a view to avoid and/or minimize incidental civilian casualties and damages. This rule would require that a commander should consider whether the same military advantage could be achieved by using CNA if this is practicable and would cause less civilian casualties or damage compared to a use of more conventional weapons. However, again, there is the challenge of estimating the damage caused by the knock-on effects of CNA on interconnected military-civilian systems. 115 AP I art. 58 (a) and (b) require a state to segregate its military assets from the civilian population and civilian objects to the maximum extent feasible. Where segregation is not feasible, the government must protect the civilian entities and communications from the effects of attacks. Due to interconnectivity between military and civilian systems, and the involvement of private contractors in the operation and maintenance of military critical infrastructure, this segregation may be infeasible. 116

This renders the protective obligation under AP I art. 58 (c) particularly important. Parties are to “the maximum extent feasible” to take “other necessary precautions” to protect civilians “under their control”. The first and the last of these limit the extent of required government action, while the second forces governments to undertake otherwise deferred action. Commentators argue that how governments interpret the content of this obligation will be central to future cyberwars. Governments need to know what to protect and the extent of the protection. Among potential measures (designated for the U.S context but applicable to other domestic setting in modified form) would be

- To regularly identify those civilian systems, networks, and industries that will become legitimate military targets in time of armed conflict because of their nature, location, purpose, or use. This also includes those that may come under the control of the government but not become military objectives.
- To determine what kind of protection should be given to privately owned industries, systems, and networks that are anticipated to come under the control of the government during times of armed conflict. Part of this authority should include methods to monitor, implement, and enforce cybersecurity and survivability measures in those specific networks, systems, and industries now. Agreements need to be made with these actors to ensure sufficient protection of industries and networks, including a system for monitoring and enforcing the implementation of protective measures.
- The potential establishment of a “hack back” solution, that is to say “active defenses” (as opposed to passive defenses, such as firewalls and virus protection) that could provide a deterrent to attacks by detecting, stopping and disabling/destroying the attackers abilities.

---

114 Schmitt, M 2002, id.
115 Dörmann, K. 2004, id.
The creation of a strategic reserve of Internet capability, including bandwidth, routers, and other necessary means which would ensure that critical cyber networks and systems have a place to go when they are being attacked.\(^\text{117}\)

### 7.5. Deceit and deception in cyber-attacks: the prohibition of perfidy

What are the rules concerning deceit and deception applicable to CNA? AP I art. 37 prohibit perfidy, that is, the feigning of protected status in order to take advantage of an adversary by leading him “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”. Only the killing, injuring or capturing of an adversary by resort to perfidy is prohibited, not physical damage caused by it. Misinformation implicating the enumerated protected persons or objects would be unlawful including pretending to be wounded or sick or have non-combatant status or surrendering and improperly displaying symbols that signify protected status, such as the Red Cross or Red Crescent.\(^\text{118}\) AP I art. 38 prohibits the misuse of protective signals and AP I art. 39 prohibits the use of the enemy’s military emblems, insignia or uniforms. Examples of perfidy in the context of CNA would be manipulating the enemy’s targeting database to believe that one’s own division headquarters were a hospital.

Importantly, perfidy is distinguished from ruses, which are acts intended to mislead an adversary and cause him to act recklessly, but which do not involve false claims of protected status. Ruses are lawful, and might include transmitting false data, meant to be intercepted by an adversary, about troop deployment or movements. Alternatively, it might involve altering data in an adversary’s intelligence databases, sending messages to enemy headquarters purporting to be from subordinate units, or passing instructions to subordinate units that appear to be from their headquarters.\(^\text{119}\)

### 7.6. Neutrality

What respect is owed to neutral states, and what must states do remain neutral? The 1907 Hague Convention regulating the law of neutrality has important implications for CNA. States that declare themselves to be neutral, and act accordingly, are entitled to immunity from attack. Cyber neutrality may be defined as the right of any state to maintain relations with all parties in a cyber conflict, and the right not to support or take sides with any cyber belligerent. Neutrality does not require neutral states to shut off all commerce with combatant states, though any provision of military aid to a combatant state during conflict is prohibited.\(^\text{120}\)

Article 1 state that “The territory of neutral Powers is inviolable”. According to article 2, belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power. There are also obligations incumbent on the neutral power, which according to article 5 must “not allow any of the acts referred to in Articles 2 to 4 to occur on its territory.” If violations of neutrality take place, the neutral power is called upon to “punish” those acts. Article 8 contains a limited exception where a state may let all belligerents use “telegraph or telephone cables,” or a “wireless

---

\(^{117}\) Talbot Jensen 2010, id.
\(^{118}\) Dörmann, K. 2004, id.
\(^{119}\) Schmitt, M 2002, id.
telegaphy apparatus” belonging to the neutral state or to companies or private individuals, to transmit signals containing intelligence, orders, or other dispatches.

Due to the structure of the internet, where internet nodes are dispersed globally, many CNA will violate the norms of neutrality in a number of ways: first, a belligerent violates neutrality law when it launches a cyber-attack across the internet nodes of a neutral state despite the lack of physical intrusion. The same applies to cyber-attacks launched from a neutral state, even if the neutral state did not control the attack. International law would appear to require a belligerent state (or third party neutral) to stop its citizens from engaging in such acts.

The prohibition on moving weapon across the territory apply to CNA: For example the United States Air Force has defined “weapons” as “[d]evices designed to kill, injure, or disable people, or to damage or destroy property.” A cyber weapon can destroy military and civilian targets. The prohibition is irrespective of the size of the weapon. This might be having the effect of drawing the neutral state into the conflict. If the neutral state cannot or does not take action to halt the attack, the opposing belligerent may choose to physically attack the neutral state’s communications infrastructure to limit or halt the cyber-attack.

Second, an additional violation may occur because the current structure of the internet makes halting these incursions extremely difficult. Hence, a neutral state may risk violating its duty of neutrality to take action to prevent the cyber-attack. Yet neutral states do not have a practical method of detecting such attacks, and even if the neutral state could detect the violation, under the existing structure of the Internet, “a state may not be able to prevent [cyber] attacks from leaving its jurisdiction unless it severs all connections with computer systems in other states.” Such interpretation would place an undue burden on the neutral state as well as leading to the disruption of legitimate Internet communications.

Hence, it is argued that the kind of difficulties belligerent and neutral states face in complying with IHL under the current structure of the Internet, the scope of the duties imposed under IHL on neutral and belligerent states should change. One approach would be to adopt an intent-based view of neutrality, where a belligerent would not violate IHL unless it intentionally directed cyber weapons through the Internet nodes of a neutral state. Here, the neutral state would not be required to take action to prevent the unintentional passage of the cyber weapons through its borders, and a belligerent could not take action against a neutral state that was unable to prevent the passage of cyber weapons through its networks. Under this view, as long as the neutral state takes no action to favor one belligerent or the other, it maintains its neutrality, and the risk of an ever-widening conflict may be averted.121

**Summary**

What particular problems arise from the application of IHL to CNA attacks? The challenge for lawyers and force planners is to identify and conduct realistic exercises where scenarios arise. However, a general problem in adapting the jus in bello for cyberwar is that lawyers lack scientific and technical skills to analyze technological developments. Moreover, research on information war is classified and thus inaccessible.122 Finally, a plethora of overlapping and competing legal regimes require states to adjust their CNAs to satisfy their obligations under various specialized regimes.

---

121 Kelsey 2008, id.
122 Haslam 2000, id.
of international law, and to negotiate the relationship between international law obligations and domestic legal norms.\textsuperscript{123}

There are also some more specific questions as to the suitability of the jus in bello regime for regulating the conduct of cyberwar. One commentator has pointed out that the higher the threshold is for acknowledging a CNA as an attack in the meaning of IHL, the more likely it is that its use against civilians and their objects is permissible, again resulting in warfare having more impact on civilians by expanding militaries’ ability to target (but not attack) them. This consequence stands in direct contrast to the notion that the law of war should protect civilians and their property as much as possible.\textsuperscript{124} A related concern is that cyber-war leads to more frequent violations of the principle of distinction, because states can use cyber weapons to attack traditionally protected objects and individuals without incurring the political cost associated with civilian casualties.\textsuperscript{125} Along the same line it is also argued that cyberspace erodes the segregation between war-space and civilian-space and that this erosion undermines the distinction between combatants and non-combatants.\textsuperscript{126}

Conversely, other commentators argue that the ability of CNAs to interrupt operations at targeted facilities (particularly those that are dual use) instead of destroying them not only limit potential troop losses but actually increases the options for minimizing collateral damage and incidental injury.\textsuperscript{127} Rather than prevent the development of these weapons, the concepts of distinction and neutrality should evolve to encourage states to use cyber weapons in some circumstances while also properly restraining their use in others. Because of the nonlethal potential of these weapons, IHL should offer states greater flexibility in deploying cyber weapons rather than regulating cyberwarfare with the same restrictive rules that apply to conventional weapons. For example, IHL could allow for the targeting of any object that provides effective war-sustaining capability or indirectly contributes to military action, regardless of whether its neutralization offers a definite military advantage.\textsuperscript{128}

\textsuperscript{123} Hollis D.B 2007 id.
\textsuperscript{124} Hollis D.B 2007 id.
\textsuperscript{125} Kelsey J.T.G. 2008, id.
\textsuperscript{127} Schmitt, M 2002, id.
\textsuperscript{128} Kelsey J.T.G. 2008, id.
Conclusion

The objective of this working paper is to present a broad perspective on the potential role(s) of law in providing a framework for governing cyber-attacks as threats to national and international security. The discussion has been situated through a four-part structure: the first part considered the regulation of cyberwar in light of empirical developments, the ongoing institutionalization of cybersecurity issues as “war” and the discursive role of law in this process. The second part explored the “inside view” where the existence of cyberwar as a threat to national and international security is taken for granted. It traced the evolution of the cyberwar discourse, and looked at the conceptual and definitional challenges that characterize the current debate. Three contemporary models for regulation were described, along with an alternative position that articulates a call for a comprehensive legal approach. The third and fourth part mapped key discussions in the jus ad bellum and the jus in bello. As stated in the introduction, the working paper aimed to achieve two things: first, to offer policy makers and the general public a comprehensive and critical introduction to the legally relevant aspects of the cyberwar discourse. Second, to unpack the role of law in the current drive to move cybersecurity issues into the domain of warfare. The working paper concludes by pointing to three observations:

First, the focus on cyberwar as threat to national security and international peace may engender a problem of misspecifying the solutions to cybersecurity issues and the future governance of cyberspace. While the effort to militarize cyberspace should be treated with skepticism, the civilian approach is also hugely problematic: Whereas international law offers a regulatory framework for a crucial but small part of the cybersecurity challenge, the lack of adequate critical information infrastructure protection and the insufficient coordination of domestic legal regimes are problems that receive insufficient policy attention most places. The comprehensive legal approach offers a promising way forward with its focus on legal coordination between fields such as information society and telecommunications, cybercrime, national security and armed conflict. Advocating for this approach may also assist military leaders in demanding more pro-active stances from government and private sector actors.

Second, the militarization of cyberspace calls for a concerted effort to promote a “cyber peace” agenda, beyond the clarification the norms of the law of armed conflict. As described in the working paper, some scholars have begun to argue that cyberwar makes war more humane, and that international law should adapt to and promote cyberwar as an alternative to traditional warfare. Taking the opposite approach, how can policy makers ensure that sufficient attention is given to how international norm-making can be part of the work to ensure “cyber-peace”? For example, in the context of the law of war, the considerations that support expanded or restrictive interpretations of “use of force” or “armed attack” will be strategic and linked to national interest. Cyber peace could be promoted by de-linking cybersecurity issues from armed force and by imposing a high legal threshold for treating them as equivalent. A different example is CNA-staffing. Due to shortage of capacity, the use of private contractors is endemic in the cyberwar field globally. Is some kind of special agreement needed on the status of these contractors?

At the same time, cyber peace should not be defined only in the negative: attention must be given to the role of international law in the development of a substantive cyber peace agenda. Some such activities already exist: For example, the Secretary-General of
the International Telecommunication Union (ITU) supports a cyber-peace initiative, which is an attempt to “delegitimize cyberwar through reversing the perspective offering a counter-narrative in a debate that tends to be dominated by terms like cyber-attack, cyber-war, or electronic Pearl Harbor”.\footnote{See Wegener, H 2011, The Quest for Cyber Peace, International Telecommunication Union and World Federation of Scientists; Wegener, H 2007, ‘Harnessing the perils in cyberspace: who is in charge?’ I Disarmament Forum vol. 3, available at \url{http://www.unidir.org/pdf/articles/pdf-art2645.pdf} (Last visited 14.03.2012).}
Towards a Militarization of Cyberspace?

Cyberwar as an Issue of International Law

The rationale behind this study is that while cyberwar is gaining recognition as a “fifth battlefield”, policy makers and the general public have insufficient knowledge about the legal and strategic implications of this development. The project explores questions of relevance for policy and public debate, such as: How can policy makers develop legal mechanisms and procedures that allow for cybersecurity threats to be properly assessed? In creating a legal regime for Cyberwarfare, what dilemmas arise? Which legal considerations and constraints should shape the development of civilian and military cybersecurity institutions? Why is a critical perspective on the cyberwar discourse important for policy making? To address these questions, the project will undertake five thematic investigations:

1. Cyberwar as an issue of international law
2. Cyberwar in the NATO Strategic Concept: Some Issues
3. Distribution of Competence between Civilian and Military Authorities
4. The Relationship between International and National Institutions
5. The State, the Market and the Role of Public/Private Partnerships in Cyberwarfare

This working paper will discuss cyberwar as an issue of international law. The working paper examines some of the legal and strategic challenges that arise with respect to the development of effective international and national strategies to prevent, regulate and resolve cyberwar.