TRANSMISSIONS: THE JOURNAL OF FILM AND MEDIA STUDIES 2017, VOL.2, NO. 1, PP. 78-99.

Ivory Mills
Northwestern University

Emergent International Humanitarian Law in the Context of Cyber Warfare

Abstract

Over the last decade, actors throughout the international community have begun to engage in information operations (IO)—the use of information technology such as computer network attacks to influence, disrupt, corrupt, usurp, or defend information systems and the infrastructure they support. Current international humanitarian law fails to address the challenges that arise from technological advancements, often lacking consideration of the many non-state actors actively involved Additionally, and arguably most importantly, it is unclear whether cyber-attacks constitute the use of force put forth in the UN Charter. Examining recent changes in technology, the increased presence of non-state actors, a decade's worth of cyber-attacks, and recent developments in domestic and international law, it becomes clear that the existing legal framework is inadequate and necessitates further consensus building and negotiation across the international community.

Key words: cyber war, international humanitarian law, information operations, information technology, cyber attacks

Introduction

As the development and pervasiveness of information and communication technologies (ICTs) continues to increase, individuals, organizations, and nations continually find new, unanticipated, and often unlawful ways to use them. Over the last decade actors throughout the international community have begun to engage in

information operations (IO) or cyber-attacks. "Information operations are the integrated employment of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supported and related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting [y]our own".[1] Computers control most infrastructure, including telecommunication networks, water supplies, electrical grids, oil storage and transport networks, banking and financial systems, and emergency services.[2] Given their widespread capabilities and scope, such computers and technological networks are ideal for use as weapons and targets of information operations.

Because the technology is mostly inexpensive, widely available, and deployable from virtually anywhere, cyber-attacks are highly attractive to state and non-state actors. Moreover, their threats and consequences are disconcerting, as they have the potential to disable a country's infrastructure, destroy financial systems and data, and disrupt national communications systems, amongst other things. But the technologies and their uses have dramatically outpaced the laws and policies that govern them in international conflict. As such, national and international governing bodies have struggled to adapt and integrate existing laws and practices to this novel phenomenon. There is continued disagreement about if and how international humanitarian law governing the use of force, *jus ad bellum*, applies to information operations. This paper explores emergent international humanitarian law (IHL) of information operations, highlighting how new technologies, recent events, and multiple stakeholders have complicated the understanding and application of IHL in this context. It discusses the opportunities and threats that have emerged and details the considerations that must be made to establish adequate and effective law to regulate cyber war in the modern, globalized, multistakeholder regulatory environment. Finally, utilizing a constructivist approach to IHL, it posits that its existing laws are inadequate for the current international system and puts forth an interdisciplinary approach necessary to address the complex challenge of developing a rule of law to govern cyber war in the international community that binds the relevant actors with mechanisms that the vested stakeholders will abide by and buy into.

[1] Joint Chiefs of Staff, Joint Publication 3-13 Information Operations (2012).
[2] Jennifer J. Rho, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695 (2007).

What's new?

Technology

The threat of cyber war is the result of the growth and development of the information society. Perhaps, the most significant aspect of the information society is the rapid and expansive development of information and communication technologies (ICTs). These technological advancements provide continuous access to information and data and unprecedented interconnection across all aspects of society. Given the history of the internet (initially developed for and by the U.S. military), it is no surprise that military organizations continue to take advantage and often lead the charge in developing and advancing ICTs, and utilizing these technologies in their strategic and tactical exploits to further national security. Additionally, cyberspace has become a critical battleground due to the economic and geopolitical implications of increased access and connectivity, and the pervasiveness and vulnerability of the technologies.

In 1969, the US military developed ARPANET, a program to facilitate communication between the Department of Defense, its contractors, and universities. As ARPANET evolved into the internet, it quickly spread to industry and the consumer public, utilizing increasingly available telecommunication mediums, such as telephone lines, microwave relays, and satellite uplinks. And as fibre optic cables, transistors, and microchips were developed, the internet and ICTs rapidly diffused throughout the world. Consequently, multiple actors (individuals, states, corporations, non-state actors) gained access to create and deploy programs, code, or mechanisms that influence, disrupt, corrupt, usurp, or defend information systems and infrastructure. Recognizing the threats resulting from these technologies, states began developing offensive and defensive cyber war technologies.

In this new battlefield, cyber weapons are classified into three categories: syntactic attacks, semantic attacks, and mixed attacks.[3] Syntactic attacks acts modify the logic of computer operating systems to introduce delays and or make the system act in unpredictable ways.[4] Examples of syntactic attacks include malicious code, denial of service, and hacking. Malicious code is a programmatic language designed to damage or infiltrate computer files and programs. Sometimes it replicates system files and has the potential to cause huge economic damage by crashing the entire host system. Viruses are files that enter a computer system and, once opened, they corruptand destroys computers, sometimes to the point of making the entire computer inoperable.[5] Lastly,

[3]Jennifer J. Rho, p.139.
[4] Jennifer J. Rho, p.139.
[5] Jennifer J. Rho, p.139.

hacking is breaking into a computer and altering its operating system by bypassing the security functions.

In contrast, semantic attacks target the accuracy of information the user has access to, which appears to the owner/operator to work be working normally.[6] Semantic attacks can utilize the infiltrated systems to control the information contained on government and military sites, and cause serious problems on connected systems. They have been used to feed false data to industries and infrastructural operations, causing a shutdown of electrical power, air traffic controls, and emergency response systems. Such disruptions on a wide scale basis could cause panic and unrest.

The isolated and combined use of syntactic and semantic attacks, which disable critical operational systems and feed disinformation, could result in numerous destructive social, political, and economic scenarios, including but not limited to critical public and private critical national infrastructures.[7] The use of new technologies in this emergent battlefield not only has significant economic and political consequences, but also the potential to cause widespread physical destruction and social unrest.

Events

In addition to, or in light of, the development of these new technologies, actors throughout the international community have found novel and often unanticipated ways to utilize the technologies in social and political realms. Consequently, as history has demonstrated, law has emerged because of a series of unfortunate events. In this case, governments, individuals, organizations, and other non-state actors have employed ICT technologies in information operations. And while there have not been any insurmountable or global cyber-attacks to date, there have been some which—for the victim states—were significant.

Israel-Hezbollah "July War" of 2006

In February 2005, Former Lebanese Prime Minister Rafiq al-Hariri was assassinated, resulting in mass protests.[8] Based on speculation that the new government

[6] Jennifer J. Rho, p.140.
[7] Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyberattacks,* 2002 U. ILL. J. L. Tech. & Pol'y 1, (2002), pp. 40-41.
[8] Paulo Shakarian, Jana Shakarian, Andrew Ruel, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (2013).

would demilitarize Hezbollah and rumours that Israel would strike Lebanon, Hezbollah took pre-emptive action, killing three and kidnapping two Israeli soldiers and launching several short-range rocket attacks against Israel. Israel responded with a massive attack, damaging a significant amount of Lebanese infrastructure and killing over 1,000 civilians, but failing to demilitarize Hezbollah. Throughout the course of these ground and air attacks, both sides used cyber war tactics to support their kinetic efforts.

The Israelis conducted denial of service attacks on Hezbollah's television station, while Hezbollah hackers allegedly gained access to the networks of Israeli Defense Force units at the Lebanese border.[9] Additionally, Hezbollah integrated a "cyber psychological operation" (CYOP) into their military strategy. CYOP is the use of cyber operations to directly attack and influence the attitudes and behaviours of soldiers and the general population.[10] With this strategy, the attackers used credible political and military power to get attention and project information power, thus shaping the information environment of the conflict.

In response to Hezbollah's CYOP, many of Israel's Western allies banned Hezbollah's websites. Unable to utilize their legitimate site, Hezbollah hijacked IP addresses of corporations around the world to ensure that their messages were successfully transmitted to the intended recipients—the general public, the Israeli public, and anti-Hezbollah individuals, organizations, or states.[11] IP hijacking transmits information from one location to another through a series of routers. This strategic manoeuvre of utilizing non-combatant IP addresses allowed Hezbollah to maintain the communication of their strategic message.

This instance creates unique and timely challenges for understanding the role of international humanitarian law in cyberwar. These attacks by Hezbollah raise the question of whether or not nonstate actors could commit acts of war?

Estonia 2007

On April 27, 2007, the Estonian government completed long-held plans to relocate a national monument. Initially installed by the USSR in 1944 to honour Soviet soldiers who died during WWII. Significantly opposed by the Russian population of Estonia, the relocation sparked a series of protests in Tallinn. Thus in 2007, Estonia became the first state victim of an overt and coordinated assault on its

[9] Paulo Shakarian…, p.78.
[10] Paulo Shakarian…, p.79.
[11] Paulo Shakarian…, p.81.

telecommunications networks.[12] At the beginning of the protests, there was an internet post in a public forum, giving instructions for participating in a distributed denial of service attacks against Estonian government systems.[13] While the riots and protests in the streets of Tallinn had subsided, on the internet there was an ongoing, multifaceted campaign of denial and disruption.

For three weeks, Estonian websites were flooded with data requests from thousands of computers in increasingly larger waves. The requests first knocked out government websites, including, but not limited to those of the Prime Minister and the President, the Justice Ministry, and the Foreign Ministry.[14] Eventually, the attacks spread to daily newspapers, broadcast television, internet service providers, hospitals, banks, universities, and public service providers, disabling emergency phones for fire and paramedic services for an hour.[15] Over a million computers were infected with botnet viruses.[16] Eventually, Estonian officials produced evidence suggesting that the Russian government was involved in these attacks. But there was little recourse for Estonia in the international community via diplomatic or legal avenues.

Iran (Stuxnet) 2010

In 2010, a 500-kilobyte computer worm was discovered as it invaded computers around the world. The virus was especially sophisticated, including a specific attack vector limited to certain computers.[17] Now commonly known as Stuxnet, the virus was used to infect at least 14 industrial sites in Iran, allowing its creators to spy on the systems and causing the machines on site to tear themselves apart, despite the efforts of their human operators.[18] Stuxnet was very precise, inflicting little to no damage on

[12] David Hollis, *Cyberwar Case Study*: Georgia 2008, Small Wars Journal (2008).
[13] Paulo Shakarian…, p.50.
[14] David Hollis, p.1025.
[15] David Hollis, p.1025.
[16] Bots and Botnets – A Growing Threat, http://us.norton.com/botnet/ , (2016). A "bot" is a type of malware that allows an attacker to take control of an affected computer. Also known as "web robots," bots are usually part of a network of infected machines, known as a "botnet", which is typically made up of victim machines that stretch across the globe. Since the bot infected computer does the bidding of its master, many people refer to these victim machines as "zombies." The cyber criminals that control these bots are called botherders or botmasters. Some botnets might have a few hundred or a couple thousand computers, but others have tens and even hundreds of thousands of zombies at their disposal. Many of these computers are infected without their owners' knowledge."
[17] John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*. J. Marshall J. Computer & Info. L. 1 (2011-2012), p.29.
[18] John Richardson, p.3.

any person, place, or system other than the target, a rarity in the context of war. Like other modern ICTs, the perpetrator's identity remains anonymous (despite continued speculation and suggestion that the United States was responsible). These distinctions are especially important when trying to understand the role of IHL in regulating cyber-attacks. Like new war technologies of the past, cyberwar technologies challenge the common notions and understandings of battle: if the perpetrator remains anonymous, who is the attack attributed to? If the attack travels around the world before reaching its target, who has jurisdiction? Because these attacks can be more precise than other weapons, do the responses have to be as exact to meet the necessity and proportionality requirements of IHL?

These attacks represent a few particularly significant instances of information operations, but are not, by any means, representative of the scope, scale, or number of attacks that have occurred.

New Stakeholders: Non-state Actors

Because of the nature of information operations, non-state actors are now empowered to exploit and undermine IHL because they make it impossible to compartmentalize the battlefield and single out with sufficient clarity who the military targets are. The law of war and the use of force have traditionally governed conflict between nation states. With the insertion of hacktivists, terrorists, and other non-traditional actors in war, it is unclear how victim states respond, who is responsible, what the consequences can and will be. There are some arenas in international law that recognize the importance of non-state actors; however, in the perpetually unresolved regulation of information operations, no such policy statements have been made by international bodies. Instead, non-state actors responsible for cyber-attacks are often considered cyber criminals, in violation of domestic cybercrimes, or even less justiciable, as nuisances.

For example, Anonymous is a collective, politically motivated hacking group with a core of highly skilled IT personnel that has demonstrated its willingness to conduct operations against government and military-affiliated Web sites.[19] The collective is featured in the media nearly every week for claiming to be or being found responsible for cyber-attacks against governments and corporations.[20] Anonymous has led efforts to publish sensitive national security information contained by government and

[19] Paulo Shakarian…, p.135.
[20] Paulo Shakarian…, p.160.

government-contracted private actors.[21] For example, the term "anti-security" refers to a movement to counter government efforts to increase cyber-security. Such information operations by individuals, hacking groups, and terrorist organizations have proven especially difficult for victim nations and corporations, since international humanitarian law applies to states and the perpetrated attacks often occur in multiple jurisdictions, by multiple people, and may not cause as much damage as the international community would deem necessary to constitute a use of force.

Resultant Debates & Issues

These technologies, events, and new actors involved in information operations have dramatically altered the regulatory landscape. They have resulted in a variety of opportunities and threats, as well as debates about utilizing, altering, or developing international humanitarian law in the context of cyber war.

Attribution

The technologies and non-state actors in the context of information operations gives rise to a long-held debate about attribution. Attribution in IHL is "the means by which responsibility for illegal acts or omissions are attached to the state".[22] There are concepts of both direct and indirect responsibility when determining attribution. Under direct responsibility, states are liable if their direct acts or omissions led to harm, if the actor acted on behalf of the state or state agent, or if the state has control over non-state actors.[23] Indirect responsibility, on the other hand, finds states liable when there is no underlying link between the actor and the state, and is often applied in the context of terrorism.[24]

International humanitarian law governs state action, and state responsibility depends on attribution. But cyber-attacks challenge the notion of attribution because the wrongful act appears to be ascribed to a computer by location; and if not the computer, then by the non-state actors, who are beyond the legal scope and definition of a state. According to the Tallinn manual, the fact that a cyber operation has its source

[21] Paulo Shakarian…, p.167.
[22] Levi Grosswald, *Cyberattack Attribution Matters Under Article 51 of the U.N. Charter*, 36 Brook. J. Int'l L. (2011), p. 1154.
[23] Levi Grosswald, p. 1154.
[24] Levi Grosswald, p. 1154.

in governmental infrastructure is not sufficient to attribute these acts to that State, but instead it constitutes an indication that a State is associated with the cyber operations.[25] In contrast, international law scholars Shackelford and Andres argue for a more flexible standard of responsibility for cyber-attacks because it is so difficult to prove the identify of attackers. These ongoing debates and the changes that shaped them lead to more questions and conversations that must be addressed legally and practically.

In determining to whom attribute a cyber-attack, security analysts look at from where (from what IP address) the software/attack came; how, when, and by whom the software was constructed; and what the software was designed to do. But answering these questions is much more challenging than it may seem, not only because the internet is so expansive, but also because cyber attackers work diligently to hide information about the origins of an attack. Even if an analyst could reverse engineer the software, the IP address could be faked or could have been rerouted through many different physical locations. Moreover, the source IP may contain malicious software that could prevent tracing or that could infect an analyst's computer, completely disrupting the investigative process.[26] Thus, victim states, corporations, and individuals can rarely, if ever, be sure that they've correctly determined the source of an information attack. Thus, unless the attacker claims responsibility, it is nearly impossible to determine with 100% certainty who is responsible for a cyber-attack.

In the Estonia case discussed above, attribution was a critical challenge to IHL and a very early demonstration of its limitations as currently conceived. The Estonian government claimed that they were victims of a cyber-attack—a novel and unregulated type of warfare by Russia; however, the international community responded with little urgency. Despite the U.S.'s position that cyber warfare is a top priority and 'fair game' in international politics, its officials wrote of the events in Estonia as a "cyber riot". Similarly, NATO's response to Estonia's calls for assistance from the international community was limited and did not provide any recourse. Besides the claims from Estonia, no state actor vocally placed blame on Russia, be it for evidentiary or geopolitical reasons. Eventually, NATO assembled a group of legal scholars and lawyers to create the Tallinn Manual to interpret how existing legal principles applied to cyber war. Nevertheless, it remained unclear to the Estonian government and the international community whether the cyber-attacks endured were regarded as an act of war that warranted a proportional response (kinetic or otherwise).

[25] *Tallinn Manual on the international law applicable to cyber warfare 2013*. (2013).
[26] Paulo Shakarian…, p. 32.

Authority

Another critical challenge in the context of modern information operations is that of authority. Essentially, the question that emerges is whether international humanitarian law has legitimate governing purview to make and impose laws in cyberspace. By definition, authority is the sense in which a person who has power can get others to act in particular ways. Practically speaking, a state is considered to have authority if it maintains public order and makes laws that are generally obeyed by its citizens.[27] While it has been widely accepted that international humanitarian law governs, is less clear how legitimate and effective its authority is on states. This becomes even less clear when looking at the undeterred and even emboldened nature of non-state actors involved in conducting cyber-attacks, as well as in the failure of the international community to come to a consensus on its modus operandi regarding information operations conducted by states against other states.

In the Israel-Hezbollah case discussed earlier, Hezbollah's hacking of the Israeli Defense Force units and their use of CYOP to shape the information environment by utilizing non-combatant IP addresses to gain credible political and military power highlights the challenges of understanding authority in this context. While Hezbollah is not a legitimate state, it has historically exercised widespread and significant military, economic, and political authority. Furthermore, it repeatedly engages in kinetic warfare. Nevertheless, as it adapts to the emerging landscape that includes cyber weapons, it still is unclear whether its (or any other terrorist organization) actions are governed by IHL. Some might argue that they have the authority to be considered a state, but many others would staunchly disagree. These debates and their continued negotiations are represented in the existing international and domestic laws detailed in the following section.

Existing law

The dynamic nature of this issue has a variety of implications and draws influence from both national and international laws and practices that lead to the development of legal norms, which—at best–continue to be ineffective and incoherent.

[27] Lacewing, Michael. *Authority and Legitimacy.* (Routledge) (2013); http://cw.routledge.com/textbooks/alevelphilosophy/data/AS/WhyShouldIBeGoverned/Authorityandlegitimacy.pdf. date accessed 28.09.2017.

International law

The biggest conflict in the debate of IO regulation is whether a cyber-attack constitutes an armed use of force. This question shapes the emergence of international law and practice because it determines if the conduct of an information operations rises to the thresholds described in the UN Charter, which in turn determines how states can act and react.

Use of force derives its meaning from the UN Charter. Article 2(4) states, "[a]ll Members shall refrain in their international relations from the threat or [armed] 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".[28] Subsequently, Article 51 articulates that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations".[29] It is generally agreed that Article 51 carves out an exception to Article 2(4)'s prohibition of force. With respect to IO, these provisions raise several questions. First, are there certain cyber-attacks that constitute a use of force as articulated by the Charter? If so, what is the distinction? Second, could a cyber-attack provide the victim state the right to use kinetic force in response, and still meet the necessity and proportionality requirements of IHL?

The Charter Articles acknowledge that national sovereignty underscores international humanitarian law.[30] When a State's conduct rises to the threshold, the law of armed conflict applies. As such, an unlawful armed use of force justifies countermeasures. But even before technology existed to facilitate information operations, not all aggressive acts would amount to an unlawful use of armed force. It is also widely acknowledged that Article 51's "armed attack" is a narrower category of actions than "use of force" and typically requires some sort of physical damage to persons or property.[31]

Customary law, guided by the Nuclear Weapons Advisory Opinion issued by the International Court of Justice, suggests that Article 2(4) applies to "any use of force, regardless of the weapons employed.[32] Additionally, Article 36 of Additional Protocol I articulates that states that develop new weapons or methods of warfare have an

[28] U.N. Charter art. 2, para. 4.
[29] U.N. Charter art.51.
[30] Priyanka R. Dev, *"Use of Force" and "Armed Conflict" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N.* Response, 50 Texas Int'l L. J. 2, (2015).
[31] Priyanka R. Dev, p.385.
[32] I.C.J. Reports 1996, p. 226.

affirmative duty to determine if its use would be prohibited.[33] Thus, it is argued that IO can be governed by analogy to existing international law of war. Despite all this, it remains unclear if, when, and how these concepts apply to information operations for a variety of reasons, including attribution, imminence, and geography.

As mentioned above, in response to the ongoing confusion, NATO formed an International Group of Experts, which set out 95 non-binding black letter rules in the *Tallinn Manual on International Law Applicable to Cyber Warfare*.[34] The manual examines how extant legal norms apply to this new form of warfare, detailing the ways international customs, as understood by these scholars, apply to cyberwar.[35]

While the manual is not a binding legal authority, its comprehensive nature does provide an authority which demonstrates how customary law could apply and provides the framework for a legitimate binding agreement. Whether it becomes enacted as law or not, it is undisputed that the *jus ad bellum* principle could apply to information operations. However, when and how it applies gives rise to another historical divide over the UN Charter's interpretation and demonstrates the challenges to building international consensus.

In addition to trying to understand the applicability of jus ad bellum to cyber war, it is important to understand how and when it applies. The dominant view among scholars is that if the effects or consequences of state-sponsored cyber intrusions are sufficiently damaging, international humanitarian law should govern and recourse to armed force may be justified against states responsible.

Professor M.N. Schmitt argues, "as the nature of a hostile act becomes less determinative of its consequences, current notions of "lawful" coercive behaviour by states, and the appropriate responses thereto, are likely to evolve accordingly".[36] He highlights the areas of uncertainty and disagreement in the legal analysis, but asserts that "attack" is a term of prescriptive shorthand meant to address the consequences.[37] The provisions of the UN Charter seek to shield protected individuals from injury or death and to protect objects from damage or destruction, so the consequences are sufficient if they cause significant human suffering, not merely diminished quality of life. U.S. policy advisor, Howard Koh, takes a similar stance, asserting that international law

[33] Hague Convention (IV) *Respecting the Laws and Customs of War on Land*, Preamble, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631.
[34] Michael N. Schmitt, *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.
[35] Michael N. Schmitt.
[36] Pauline C. Reich, Stuart Weinstein, Charles Wild & Allan S. Cabanlong, *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity*, 1 European Journal of Law and Technology 2, (2010), p. 23.
[37] Pauline C. Reich…, p. 23.

principles apply to cyber war and, under some circumstances, can constitute a use of force within the meaning of Article 2(4).[38]

National Laws

While international law continues to be a contentious topic and its application to cyber war is unresolved, the division over the Charter's interpretation becomes increasingly clear in the development of national policies and practices. Many states have developed policies for information operations that in one way or another determine when another government's cyber operations constitute an armed use of force and legally justify a response. In 2012, the UN Institute for Disarmament Research found that 114 of 193 states have developed national cyber-security programs.[39] Of these programs, 47 include a role for the armed forces, with 12 of the 15 largest spenders having or developing cyber warfare units and 10 developing offensive cyber warfare capabilities.[40]

These policies and practices serve as important sources of law for the individual states, but also help shape the emerging international response since repeated practices over time can form customary international law.[41] Thus, the strategies these state actors employ in their development and implementation drives the development of law. "Strategy generates reappraisal and revision of law, while law itself shapes strategy".[42]

Unites States

Historically, the US and its allies have understood Article 2(4)'s prohibition of force and Article 51's right to self-defence to apply to military or armed violence.[43] However, the emergent US views lie in the middle of the traditional debate, as they try to account for the destructive potential of cyber operations without dramatically

[38] Harold Hongju Koh, *International Law in Cyberspace (2012),* http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers, date accessed 28.09.2017.
[39] UNIDIR, The Cyber Index: International Security Trends and Realities (2013).
[40] UNIDIR, The Cyber Index: International Security Trends and Realities (2013).
[41] Priyanka R Dev, p. 381.
[42] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 426–37 (2011).
[43] Matthew C. Waxman, p.427.

expanding the Charter's scope.[44] There are obviously a variety of interests competing for prevalence in the US approach: military capabilities, civilian infrastructure, the private sector, intelligence collection, and international cooperation.

In efforts to balance these interests, the US Department of Defense's (DoD) Law of War Manual XVI details its national approach and understanding of existing international principles. This document asserts, "as a doctrinal matter, DoD has recognized cyberspace as an operational domain in which the armed forces must be able to defend and operate, just like the land, sea, air, and space domains".[45] Further, it articulates the following policies, which seemingly interpret and integrate customary international law into domestic law:

"When no more specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during cyber operations in armed conflict."[46] The DoD claims that the law of war anticipates technological innovation, including cyber operations so cyber operations may in certain situations constitute a use of force within the meaning of Article 2(4). It defends this position by analogizing the effects resulting from information operations to those of kinetic operations. Essentially, if the effects of cyber operations are regarded as a use of force if resulting from kinetic warfare, it can be regarded as a use of force.[47] Additionally, a state's right to self-defence, recognized in Article 51, may be triggered by cyber operations that amount to armed attack or imminent threat thereof.

Furthermore, the U.S. is considering a cyber-security strategy that may include anticipatory cyber-strikes, designed under certain circumstances to knock out adversaries' computer systems and networks perceived as hostile. This strategy suggests that in addition to the more traditional military defence and deterrence strategies just described, the U.S. government may also be considering legal interpretations flexible enough to permit its own offensive cyber-operations below a certain threshold or against inchoate hostile cyber-activities.

In addition to these policies, the U.S. has demonstrated its interest and priorities in practice by militarizing its response to cyber-attacks through Cyber Command, bringing together the cyber components of the Navy, Marine Corp, Army and Air Force into a unified command structure.[48] These policies and practices highlight the national interests—interests that will undeniably shape emergent international law since the US is working internationally to clarify how these principles apply to information

[44] Matthew C. Waxman, p.427.
[45] The US Department of Defense law of war manual: an update. (2015).
[46] The US Department…, p.996.
[47] The US Department…, p.998.
[48] [48] Carmen-Cristina Cirlig, *European Parliamentary Research Service, Cyber defence in the EU Preparing for cyber warfare?* PE 542.143 (2014).

operations. As described by Robert Keohane and other liberal institutionalists, this is an example of powerful states creating laws that suit their interests and attempting to set an international agenda that aligns with said interests. However, because there is no single hegemonic nation in the world (despite the pervasive military capabilities of the US), to date there has not been sufficient buy-in to make this effective and legitimate law or practice.

European Union

Almost all European Union member states have adopted a national cyber security strategy or mention it as an aspect of their national security strategy, putting structures in place to deal with cyber threats.[49] Fifteen member states include a military perspective of cyber defence, but only a few admit to investing in cyber war technologies. In 2011, cyber defence was included among the policy priorities of the European Defence Agency and, in 2012, member states agreed to using the military to lead cyber defence efforts.

In Denmark's Defence Agreement for 2013–2017, it establishes a Centre for Cyber Security and strengthens its cyber warfare capabilities to be able to execute both offensive and defensive military operations in cyberspace.[50] In 2013, Finland announced that it would develop cyber-defence weapons, create comprehensive cyber defence capability, and establish a cyber defence unit.[51] France's 2011 strategy contains strategies to become a global power in cyber defence, safeguard its ability to make decisions through the protection of sovereignty information, strengthen the security of its critical infrastructure, and ensure security in cyberspace.[52] Furthermore, France has developed offensive and defensive capabilities and has units within its armed forces focused on both cyber war and defence.[53]

Russia

Strategically, Russia has asserted its interest in cyber warfare, stating that "by using information warfare methods to attack an adversary's centres of gravity and

[49] Carmen-Cristina Cirlig, p.6.
[50] Defence Agreement for 2013-2017.
[51] Defence Agreement for 2013-2017.
[52] France's Information Systems Defence and Security (2011).
[53] Supra note 54, p.7.

critical vulnerabilities it is possible to win against an opponent, military as well as politically, at a low cost without necessarily occupying the territory of the enemy".[54] Its Military Doctrine of 2010 notes the importance of information warfare during the initial phase of a conflict to weaken the command and control ability of the opponent and in the form of an information campaign during the actual battle to create a positive view within the international community.

China

According to Chinese scholar, Li Zhang, the Chinese stance is that the current UN Charter and other existing laws of armed conflict apply in cyberspace.[55] But how to apply jus ad bellum may require the creation of new rules or the revision and clarification of existing international rules so that they can apply in cyberspace. China highlights the novelty of the technology and the trends of the international community in its considerations.[56] Furthermore, China has invested in personnel and information infrastructure for cyber warfare. Moreover, in addition to People's Liberation Army's (PLA) operators, PLA's Unit 61398, there is a large network of volunteer Militia Information Technology Battalions, or 'net militia units', recruited from civilian talent pools.[57]

This discussion highlights the varied perspectives and approaches nations are taking to deal with this new issue. Some of which are limited to national law, while others reference, translate, or disavow IHL. These policies and practices demonstrate the interests and actions of individual nations, but also shape international humanitarian law through diplomacy and international relations. Still, there is no rule of IHL or consensus across nations that provides recourse and enforcement for acts of cyber war that have, and will continue to occur.

Towards a Legitimate IHL

Both scholarly debates and responses to recent events suggest existing international humanitarian law does not adequately regulate information operations:

[54] Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations (2010).
[55] Li Zhang, *A Chinese Perspective on Cyber War*, International Review of the Red Cross (2012).
[56] Li Zhang, p.804.
[57] Supra note 54, p.5.

they do not fit the phenomenon, their translations create uncertainty, and they lack enforcement mechanisms. Most notably, however, the existing laws are inadequate because they don't definitively identify a rigidly defined problem based on consensus building and negotiation across the international system. These failures make it impossible to determine what the law is, when actions can constitute a use of force, and what the legal response is.

The Role of Law

Developing effective and legitimate IHL to govern cyber warfare seems nearly impossible when considering the history of international law, the complexities that have arisen in the current system, and the characteristics of the internet. Despite this however, there is a necessary void that IHL must consider and fill, based on the role of law as a social construction that is larger than existing liberal institutions, and that must adapt and evolve as necessary.

Law is manmade. It is a social construction that serves the needs and desires of those who make it.[58] It is a mechanism of control and a tool of social organization, allowing the community to which it belongs to express what is just and right and to punish and/or criminalize what is wrong, unwanted, or unacceptable.[59] It determines the way its constituents behave and details the minimum standards of behaviour of an individual in his/her interactions with others in the community.[60] It works to support human and societal desires for certainty, security, predictability, and stability by providing rigid and defined standards[61]; however, it is also malleable, able to be adjusted as morals, values, needs, and times change within the realm that it serves.

International law consists of the rule of conduct for states in their relations with other states. Most notably, in distinction from national laws, it is only binding if nations accept it because the notion of sovereignty implies freedom from control and irresponsibility for action. In international law, there is no centralized authority or control over the entire community, so "in too many cases, both international law and international legal procedures are either ignored by states or are distorted by the parties to further their own interest".[62]

[58] Supra note 54, p.117.
[59] Supra note 54, p.117.
[60] Supra note 54, p.118.
[61] Supra note 54, p.118.
[62] Supra note 54, p.127.

In the context of cyber war, the role of law seems to get lost in conversations about all that is new and changing. First, in this context, which has always lacked stability and clarity, the law can serve to establish standards. Throughout history, law has served as a guide for minimally acceptable behaviour. While the various stakeholders involved in cyber war prevention and enforcement all work toward the same goal, because there is no widely accepted or binding agreement of what constitutes cyber-attacks, they are all working from different starting points and with different understandings. By establishing a standard, law can harmonize the terminology used across the international community, as well as the efforts and foci of enforcement. To date, several nations have worked to set an agenda for regulating cyber war and information operation for the international community, as liberal institutionalists would argue must occur. None have succeeded. Until there is consensus between these disjointed national approaches that thoroughly identifies and legitimizes the problem, the novelties of the technologies and the actors will continue to limit the efficacy of IHL.

In addition to establishing standards for behaviour and harmonizing terminology across the international community, the next most crucial component of an effective IHL response to information operations is compliant state action. As demonstrated in the discussion of national laws in part III, states have already begun to put forth their understanding of how IHL applies in the context of cyber war; as states continue to make policy statements and respond to threats and challenges, the scope and scale of IHL will become clear.

Compliance with the Law

In addition to states putting forth their customary practices and policy statements, one more concern within this discussion is whether states will comply with this emergent international humanitarian law. According to Louis Henkin's How Nation's Behave, "almost all nations observe all principles of international law and almost all of their obligations almost all of the time".[63] In addition, scholars of international law and relations have substantiated this claim using empirical studies, which tend to confirm "not only that nations obey international law most of the time, but also that, to a surprising extent, even the noncomplying gradually come back into compliance over time with previously violated international legal norms".[64] Even as the

[63] Louis Henkin, *How Nations Behave*. 2d ed. (Columbia University Press) (1979), p. 47.
[64] Harold Koh, *Why Do Nations Obey International Law?* Faculty Scholarship Series. Paper 2101, http://digitalcommmons.law.yale.edu/fss_papers/2101, (1997).

international community has dramatically transformed, international customs are still largely obeyed.[65]

Scholarship suggests that despite the changes, developing technologies, and broadened scope of stakeholders, compliance is still likely because it results almost entirely from the functional benefits it provides; most agree that a functioning and peaceful international society is much more beneficial than a belligerent one. Harold Koh's exploration of why nations comply with international law includes discussion of changing landscapes, actors, and technologies.[66] He suggests that in transnational legal processes, public and private actors interact to make, interpret, internalize, and enforce rules of transnational law, concluding that compliance with international law is more than likely to occur, even as everything around it seems to change. Thus, once consensus building occurs and the national and international communities agree, IHL will be more legitimate, more efficacious, and the community will be more likely to comply.

Conclusion

New technologies, recent events, and non-state participation have increasingly complicated the understanding and application of IHL in the context of cyber war. It is these new developments—coupled with international and national policies—that work collectively to negotiate emergent IHL and to determine whether, to what extent, and in what instances information operations constitute a use of armed force and how IHL applies. While this emergent law will come into being in contentious fashion (as consensus building often does), it will be binding and legitimate, encouraging most, if not all, to eventually comply.

References:

Brenner, Susan W., and Marc D. Goodman. "In defense of cyberterrorism: An argument for anticipating cyber-attacks." *U. Ill. JL Tech. & Pol'y* (2002): 1.

Center, Joint Warfighting. *Joint Task Force commander's handbook for peace operations*. Books Llc, 2012.

Charter, U. N. "Charter of the United Nations." *June* 26 (1945): 59.

[65] Harold Koh, p. 2601.
[66] Harold Koh.

Cirlig, Carmen-Cristina. *Cyber Defence in the EU: Preparing for Cyber Warfare?*. European Parliamentary Research Service, 2014.

Dunlap Jr, Charles J. "Perspectives for cyber strategists on law for cyberwar." *Strategic Studies Quarterly* 5 (2011): 81.

Eichensehr, Kristen. "Cyberwar & International Law Step Zero." (2015).

Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations (2010).

Finland National Cyber Security Strategy (2013).

Foltz, Andrew C. *Stuxnet, Schmitt Analysis, and the Cyber Use of Force Debate*. Air War College Maxwell Air Force Base United States, 2012.

Grosswald, Levi. "Cyberattack Attribution Matters Under Article 51 of the UN Charter." *Brook. J. Int'l L.* 36 (2010): 1151.

Hague Convention (IV) Respecting the Laws and Customs of War on Land, Preamble, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631.

Hathaway, Oona A., et al. "The Law of Cyber-Attack'(2012)." *California Law Review* 100: 817.

Henkin, Louis. *How Nations Behave*. 2d ed. (Columbia University Press) (1979).

Henkin, Louis. "International human rights as rights." *Cardozo L. Rev.* 1 (1979): 425.

Hoffmann, Stanley. "International systems and international law." *World Politics* 14.1 (1961): 205-237.

Hollis, David, *Cyberwar Case Study*: Georgia 2008, Small Wars Journal (2008).

Joint Chiefs of Staff, Joint Publication 3-13 Information Operations (2012).

Jonasi, Lucky. "A critical analysis of the applicability of international humanitarian law in the context of cyber warfare." (2014).

Kaiser, Robert. "The birth of cyberwar." *Political Geography* 46 (2015): 11-20.

Kelsey, Jeffrey TG. "Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare." *Michigan Law Review* (2008): 1427-1451.

Keohane, Robert O. "International institutions and state power." *Essays in International Relations Theory, Boulder, Colo* (1989).

Keohane, Robert O., and Lisa L. Martin. "The promise of institutionalist theory." *International security* 20.1 (1995): 39-51.

Kerschischnig, Georg. *Cyberthreats and International Law*. Eleven International Publishing, (2012).

Kirchner, Stefan. "Distributed Denial-of-Service Attacks Under Public International Law: State Responsibility in Cyberwar." *IUP Journal of Cyber Law* 8 (2009).

Knake, Robert K. *Internet Governance in an Age of Cyber Insecurity*. No. 56. Council on Foreign Relations, (2010).

Koh, Harold Hongju, *International Law in Cyberspace* (2012), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers, date accessed 28.09.2017.

Koh, Harold Hongju. "Why do nations obey international law?." (1997): 2599-2659.

Lacewing, Michael. Authority and Legitimacy. (Routledge) (2013); http://cw.routledge.com/textbooks/alevelphilosophy/data/AS/WhyShouldIBeGoverned/Authorityandlegitimacy.pdf. date accessed 28.09.2017.

Priyanka R. Dev, "Use of Force" and "Armed Conflict" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response, 50 Texas Int'l L. J. 2, (2015).

Quigley, Kevin, Calvin Burns, and Kristen Stallard. "'Cyber Gurus': a rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection." *Government Information Quarterly* 32.2 (2015).

Reich, Pauline C., et al. "Cyber warfare: a review of theories, law, policies, actual incidents–and the dilemma of anonymity." *European Journal of Law and Technology* 1.2 (2010).

Rho, Jennifer J. "Blackbeards of the twenty-first century: Holding cybercriminals liable under the alien tort statute." *Chi. J. Int'l L.* 7 (2006): 695.

Richardson, John. "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield." *J. Marshall J. Computer & Info. L.* 29 (2011): 1.

Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to cyber-warfare: A multidisciplinary approach*. Newnes, 2013.

Tallinn Manual on the international law applicable to cyber warfare 2013. (2013).

Tsagourias, Nicholas. "Cyber attacks, self-defence and the problem of attribution." *Journal of Conflict and Security Law* 17.2 (2012): 229-244.

UNIDIR, The Cyber Index: International Security Trends and Realities (2013).

US Department of Defense law of war manual: an update. (2015).

Waxman, Matthew C. "Cyber-attacks and the use of force: Back to the future of article 2 (4)." (2011).

Zhang, Li. *A Chinese Perspective on Cyber War*, International Review of the Red Cross (2012).