Practical Regulations of International Cyberspace

Alexis Watson

Department of English, University of Tulsa

ENGL 3003-02: Writing for the Professions for Engineering and Computer Sciences

Abigale Mazzo, MFA

November 19, 2024

Practical Regulations of International Cyberspace

The discovery and use of nuclear weapons marked a dramatic shift in international relations and just war theory. These new weapons were capable of a previously unthinkable level of damage, instantly wiping out massive cities and rendering the area unlivable for decades. Nuclear capabilities, primarily developed by the adversarial United States and Soviet Union, founded the basis for the modern peacekeeping organization of the United Nations and *détente*, or easing of strained relations. With the new global government, and the technologies that justified it, came a new way of understanding international relations as a whole; modern developments ushered in modern ways of framing State interactions. Post-nuclear theories of deterrence like mutually assured destruction and frameworks of the law of war like hegemonic stability theory are being applied to cyberspace, where they are entirely ineffective. Instead of adapting existing ideas to fit cyberspace, a domain like no other, a humanitarian framework similar to those of biological and chemical weapons should be adopted by States and enshrined in law under the United Nations.

Nuclear weapons were at the forefront of military operations and legal scholarship following the devastation of the Second World War, and with this massive power came developments in international relations that set out to understand and limit just how dangerous these weapons could be. Never before had it been so easy to cause so much harm; the push of a button would almost instantly kill millions and render thousands of square miles uninhabitable for decades. Clearly something has deterred nations such as the United States and Russia (previously the Soviet Union) from destroying each other and the rest of the world. This is laid out in the most prevalent deterrence theory: mutually assured destruction (MAD). MAD originates from the former United States Secretary of Defense Robert S. McNamara's 1960s

notion of assured destruction: “Assured Destruction involves the maintenance on a continuous basis of a highly reliable ability to inflict an unacceptable degree of damage, even after absorbing a first strike, upon any single aggressor or combination of aggressors, independently of warning, and at any time during the course of a strategic nuclear exchange” (2001, Document 103). MAD holds that the use of nuclear weapons is not feasible in a war against near-peer adversaries, since they could just as easily send nuclear weapons in return. Hence it can be understood why such weaponry is not actively in use: a nation does not want to destroy itself purely for the sake of destroying another. Another major theory that arose after the United States’ use of nuclear weapons is hegemonic stability theory (HST). HST is a theory pertaining to international security relations that posits that global security can be promoted by a single State willing to act as the hegemon, or leading role model, for the others. Nuclear weapons provide a perfect example of HST in action; the United States maintained access to nuclear weapons, yet its purposeful failure to use such inhumane and destructive capabilities showed other countries, like the Soviet Union and France, that the utmost discretion is to be kept surrounding such weapons. However, these theories found their first major challenge in the 2000s with the claim that terrorist organizations from the Middle East had access to weapons of mass destruction (WMDs). MAD was unable to function to its fullest extent since these organizations were distributed across several nations and were largely hidden, mitigating the risk of retaliation if they were to send WMDs to the United States or European countries. While MAD is functional when considering large States at war or who are hostile towards each other, and HST is functional when a State is willing to restrain itself, the ability and desire for individuals, distributed organizations, or major States to use the weapons puts intense strain on the theory.

The history of cyberattacks, and cyber warfare, is short and dense; the first widely known cyberattack is the Morris worm from 1988. The Morris worm differs significantly from the criminal or combative cyberattacks that often permeate the news in the 2020s; the Cornell graduate student Robert Morris wrote it with no malicious intent yet it wreaked havoc across thousands of computers. However, his work was able to function as a proof-of-concept for individuals and governments seeking to deal damage and commit fraud. In 2000, when only a few high-profile cyberattacks had been carried out by individuals and criminal organizations, then-President Clinton noted the potential dangers of this emerging weapon: "Yet, someone can sit at the same computer, hack into a computer system and potentially paralyze a company, a city, or a government" (Clinton, 2000, p. 14). This potentiality was realized with the cyberattack on Estonia in 2007. A small group of Russian hackers, with the support of the Kremlin, executed a distributed denial-of-service attack on the Estonian government. This brought Estonian government functions and companies screeching to a halt as almost all its internet was unusable. The next major act of cyber war was the 2010 Stuxnet attack, where the United States and Israel deployed a piece of malware on Iranian nuclear centrifuges which caused massive losses of research and energy production for Iran and surrounding countries. Since then, the number and power of cyberattacks has risen to the level of the 2021 Colonial Pipeline attack by the criminal organization DarkSide, which led to the devastation of petroleum and natural gas availability along the United States' eastern coast. The significance of indirect damages and deaths that can be caused by cyberattacks, as demonstrated throughout the past few decades, almost rivals those directly caused by nuclear weapons.

Cyber warfare is entirely unlike conventional kinetic warfare because of the unbalanced and widespread access to powerful weapons, meaning that a post-nuclear framework no longer

applies. The single potential for an individual or small group to cripple entire States' physical or digital infrastructure is enough to invalidate most post-nuclear law and war theory. Equal retribution is impossible on such a drastic level; the destruction of even a small town is far less impactful than the destruction of a major country. Authors Kumar and Nagar analyze the shortcomings of existing cyber threat models against non near-peer adversaries in their paper, "Threat Modeling for Cyber Warfare Against Less Cyber-Dependent Adversaries," and propose a new threat model that would apply to scenarios involving an uneven playing field. Additionally, authors Rovner and Moore look at how cyberspace is commonly understood like other domains and state the failures of such an understanding in their 2017 article "Does the Internet Need a Hegemon?" They argue that the Internet is unable to facilitate HST due to its distribution and due to the fact that no country is able or willing to act as a strong hegemon, not launching attacks on other nations. This is also the same reason why MAD cannot apply in cyberspace; the better-equipped countries are just as hostile as a single person because of cyber warfare's simultaneous potency and accessibility. The rapid development of cyberattacks, combined with how dangerous they can be, leads many military leaders and legal scholars to attempt to squeeze cyber warfare into existing frameworks and law of war theories that are unfit for interpreting such dangerous weapons.

Explicit post-nuclear framing, such as MAD and HST, cannot be cross-applied to cyberspace, but this does not stop some States that are resistant to change from attempting to use interpretations of existing laws instead of creating new laws like the unique cyber domain requires. The current framing, treating cyber weapons as a WMD and trying to enforce restrictions on them through existing laws, has had some successes and many failures with interpreting and explaining State behaviors from the past two decades. Furthermore, international

governmental bodies have not agreed on any particular statement or treaty regarding just how cyberspace should be understood. The North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) invited the International Group of Experts, some of the most well-read and highly experienced legal scholars and technical practitioners available, to write a treatise on the application of conventional law of war to cyberspace, culminating in the 2013 *Tallinn Manual* (Schmitt, 2013). In this first work, they analyze how current understandings of *jus in bello* (right conduct in war) and *jus ad bellum* (right to war) apply to certain cyber warfare principles. They establish black-letter rules which still stand as the most comprehensive explanation of existing international laws' applications to cyber warfare actions. A second International Group of Experts was called together in 2017 to write an updated *Tallinn Manual 2.0* that focuses on other types of cyber operations and adjusts some cyber warfare rules in light of attacks that had occurred since the first manual (Schmitt, 2017). None of the rules from these manuals have been adopted by international governmental bodies; in fact, the United States is opposed to further international regulation of cyberspace, while China and Russia advocate for new laws. In addition to the interpretations of existing international law put forth by the International Groups of Experts, Rovner and Moore explain how theories and frameworks such as the ideas of cybersecurity as a public good and HST in the Internet are currently understood. They outline the positive reasons for understanding cybersecurity as a global public good, and thus necessitating humanitarian protections, while also explaining multiple reasons why HST is irrelevant in cyberspace (2017): no State is willing to act as a hegemon by not using cyberattacks against another, cyberspace is extremely widely distributed and cannot be contained within strict boundaries, almost anyone with a connection to the Internet can launch a crippling cyberattack against anyone else, and cybersecurity itself is a public good

that should not be available for exploitation. Another author, Bu, analyzes the Huawei sanction to address the impact that non-traditional deterrence may have in cyberspace (Bu, 2024, pp. 284, 297). He states that sanctions and other economic and political acts provide an unprecedented deterrent to cyberattacks, something that is incompatible with most post-nuclear theories. It is clear, then, that common post-nuclear frameworks and even particular adaptations of them are unable to properly incorporate the significant structural and cultural differences of cyberspace.

American cybersecurity and legal experts have recently advocated for a new, and necessary, approach to framing cyber warfare by emphasizing the notion that cybersecurity is a public good and thus requires explicit protections against its exploitation. In *Rethinking Cyber Warfare*, R. David Edelman provides one of the most comprehensive frameworks for restructuring how States view and respond to cyber warfare. Rather than making further adaptations to existing and ineffective frameworks, he calls for a complete system overhaul. He rightly advocates for a broad humanitarian approach to understanding cyberattacks and their consequences, drawing analogies between cyberattacks and chemical and biological weapons. In this situation, a humanitarian framework looks at those rights which are considered to be inherent to all as public goods, such as breathable air, water, food, and land. Chemical and biological weapons are banned under a humanitarian framework because they violate the air and spread without discretion for geological boundaries or borders, much the same way that cyberattacks do. When one considers the raw power of cyber weapons, combined with the indiscriminate nature of cyberattacks and the fact that "cybersecurity is a global public good" (Rovner & Moore, 2017, p. 184) it becomes incredibly clear that cyber warfare has a much greater impact on the humanity of combatants and civilians worldwide and thus justifies a humanitarian framework to protect the rights of all. He also includes a commentary on

"structural prohibition" that notes the other factors that are at play when considering what restrains cyber war (Edelman, 2024, ch. 8). This is similar to Bu's close reading of the Huawei sanction, lending further credence to the idea that the raw power of cyberattacks is not alone enough to scare States or individuals away from using such tactics. Edelman also incorporates some ideas found in Rovner and Moore, such as the failure of HST in cyberspace and the qualities resembling those of public goods that cybersecurity possesses. While Edelman proposes strong concepts and reasoning to justify them, he does not provide much particular guidance on how these new ideas would be implemented and what they would look like. While it is necessary that a humanitarian framework is adopted when considering cyberattacks, it is also necessary to consider the practical applications of such a concept.

Although no large or comprehensive treaties regulating cyber weapons in war have been introduced or ratified, there is a clear and relevant avenue already outlined by the United Nations to create such treaties. The few works that have been written on the topic are broad and largely speculative, and none have been put into effect. This is simultaneously a good and a bad thing: the good part is that it is easier to incorporate new ideas that are more functional, while the bad is that there are currently no real laws regarding State behavior in cyberspace, thus allowing for drastic uses of force to go unpunished. The most productive method for approving such legislation is cooperation with the United Nations' Open-Ended Working Group on Information and Communications Technologies (UN OEWG on ICTs). By utilizing a similar method to the Geneva Protocol, the UN could establish a functional legal system to deal with cyberspace, thus eliminating the Wild West-like nature it currently maintains. Other organizations, such as NATO, have written out some guidelines of their own, largely based off of the manuals from Tallinn that are proving to effectively legislate cyber warfare. These guidelines should be rethought under

Edelman's humanitarian framework to consider his and Bu's understanding of structural deterrence and incorporated through the standard means of these international governmental organizations.

The United States and many of its allies are attempting to apply post-nuclear deterrence theories and frameworks of war theory, like mutually assured destruction and hegemonic stability theory, to cyberspace, which renders these old ways of understanding international relations and power dynamics useless. Instead, cyberspace and cyber weapons justify the adoption of a humanitarian framework, similar to chemical and biological weapons, and the introduction and ratification of laws under the United Nations that restrict the use of cyber weapons in all scenarios. The realization of newer and more powerful weapons technologies often shifts international law and war theory; guns reimagined war as a concept, submarines permanently redefined naval warfare, nuclear weapons recontextualized a State's valuation of life and territory.

References

Bu, Q. (2024). Behind the Huawei sanction: national security, ideological prejudices or something else? *International Cybersecurity Law Review*, *5*, 263–300. SpringerLink. https://doi.org/10.1365/s43439-024-00112-6

Clinton, W. J. (2000). Remarks on the National Plan for Information Systems Protection and an Exchange With Reporters. *Public Papers of the Presidents of the United States*, *William J. Clinton, 2000–2001*(Book I), 13–15. United States Government Publishing Office. https://www.govinfo.gov/content/pkg/PPP-2000-book1/html/PPP-2000-book1-doc-pg13-2.htm

Edelman, R. D. (2024). *Rethinking Cyber Warfare: The International Relations of Digital Disruption*. Oxford University Press. https://doi.org/10.1093/9780197509715.001.0001

McNamara, R. S. (2001). 103. Draft Memorandum From Secretary of Defense McNamara to President Johnson (D. S. Patterson, Ed.). *Foreign Relations of the United States, 1964–1968*, *X*(National Security Policy), Document 103. United States Government Printing Office. https://history.state.gov/historicaldocuments/frus1964-68v10/d103

Rovner, J., & Moore, T. (2017). Does the Internet Need a Hegemon? *Journal of Global Security Studies*, *2*(3), 184–203. Oxford Academic. https://doi.org/10.1093/jogss/ogx008

Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524