Controlling Cyberwarfare

International Laws of Armed Conflict and Human Rights in the Cyber Realm

by

William James Jordan

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Philosophy

Waterloo, Ontario, Canada, 2021

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Col. David Barnes Professor, Department of English and Philosophy United States Military Academy
Supervisor:	W. Mathieu Doucet Associate Professor, Department of Philosophy University of Waterloo
Internal Member:	Brian D. Orend Professor, Department of Philosophy University of Waterloo
Internal Member:	Patricia A. Marino Professor, Department of Philosophy University of Waterloo
Internal-External Member:	Veronica M. Kitchen Associate Professor, Department of Political Science University of Waterloo

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Cyberwarfare, military activities in cyberspace conducted by a state against another state and intended to disrupt or destroy computing or communication systems or data, is a recent addition to the warfaring arsenal. The international laws of armed conflict set out an obligation for states at war to protect civilians from the effects of the conflict. As societies continue to expand their activities in the cyber realm, the risk of cyberwarfare negatively affecting the civilian population increases. The international community, recognizing this risk, is engaged in a political dance trying to identify the constraints that international law already places on cyberwarfare while staking out ground to preserve its effectiveness as a means of influencing other states' policies. This dissertation project addresses some of the problems posed by the use of computing and network technology as weapons and targets in the context of international armed conflict. It brings together material drawn from computing technology, military handbooks, policy research, international standards for records preservation, non-government organizations, international humanitarian law, international human rights law, the international laws of armed conflict, and real-world examples to reveal the complexity and nuances of using operations in cyberspace to produce effects in *meatspace*, the physical world of humans, buildings, equipment, and artefacts.

First, I argue that since there is no significant difference between using cyber means of war and conventional means of war, it is appropriate to treat developments in cyberwarfare under the existing international laws of armed conflict. Then I introduce the *Tallinn Manual*, a handbook on the international law applicable to cyber operations, and the events that led to its development. I examine how well the *Tallinn Manual* documents the protections, prohibitions, and permissions extended under the laws of armed conflict, concluding that it is a faithful interpretation of international law.

The application of international law to warfare is always messy and imprecise. Its application to cyberwarfare is no different. This does not mean that the constraints of international law are without value or purpose. On the assumption that no state wants to start an international armed conflict, but is prepared to respond to uses of force, I apply some of the principles expressed in the *Tallinn Manual* to establish qualitative assessments of the severity of initial aggressive cyberoperations against a state, classifying them

as moderate or flagrant attacks depending on the harm they produced. This helps the target state determine whether there is just cause for a use of force, either cyber or conventional, in response, and the constraints that apply to any response that may be permissible under international law.

International law also affords protections for human rights, both in peacetime and during times of conflict. I argue that cyberwarfare exposes more civilian objects, including objects of cultural significance and records needed to safeguard human rights, to harm through both conventional and cyber attacks. If human rights are to be protected, the records (digital or otherwise) that serve as evidence in support of rights claims must be protected as well. I conclude that international law already sets out the obligation for these protections, but the interpretation of international law must make explicit the expectation that all parties in an armed conflict will make efforts to identify and preserve these objects for the well-being of persons in a post-conflict society.

Finally, I demonstrate the breadth and applicability of further work in this area. I point out some other problems that branch off from this particular project: the separation of information content from its representation in different media, human rights in the cyber domain, the use of computing and communication technology to produce social or economic disruption, the status of privately-owned satellites under the multiple international treaties and conventions during times of armed conflict, and the assignment of peacetime responsibility for safeguarding data essential for the protection and provision of human rights.

Acknowledgements

The journey from burned-out software designer to doctoral candidate in philosophy has been a long one. Along the way I have benefitted from the encouragement (and only rarely the kind from a metaphoric boot), support, and advocacy of more people than I can mention here.

I am grateful to Shelly Jordan, my wife and friend. Shelly introduced me to philosophy while she was a graduate student at the University of Calgary. Richard Zach and Elaine Landry (now at University of California, Davis) showed me that I, too, could learn to do philosophy, and the conversations I had with them and Marc Ereshefsky led me to consider doing graduate studies. Elaine specifically pointed me to Waterloo as the place to explore my philosophical interests. Jeremy Clark (University of Canterbury) encouraged me to start this journey sooner rather than later. I had no idea what I was in for, but I am glad that I did this.

The department at Waterloo has been wonderful. Tim Kenyon (currently at Brock University) and Dave DeVidi took a chance on admitting this latecomer to philosophy. They also advocated for me during a time of deep personal struggle. Dave supervised my research area in logic and, with Matt Doucet, coached me through the research area in cyberwar. Brian Orend's lunchtime talk on cyberwarfare, coming on the heels of the Stuxnet and Flame attacks, inspired the research area and this dissertation. Patricia Marino, Shannon Dea (now at the University of Regina), Doreen Fraser, Carla Fehr, Richard Holmes, and Joe Novak have all helped me stay afloat during times of potential disaster. For these I thank them, and I hope I have not disappointed them too badly.

I acknowledge the generosity of the donors to the University of Waterloo and the Department of Philosophy for the conference travel awards and dissertation completion award.

The conversations and friendships with graduate student colleagues Andria Bianchi, Tracy Finn, Nathan Haydon, Eric Hochstein (University of Victoria), Kurt Holukoff, Ashley Keefner, Catherine Klausen, Ian MacDonald, Kirsten MacDonald, Dylon McChesney, Micheal McEwen, Andrew Morgan, Corey Mulvihill, Ben Nelson, and Angella Yamamoto will not quickly fade. Thank you for the laughter and encouragement.

Greg Andres has been a great friend and mentor in pedagogy. I am not sure that I am forgiven for convincing him to lead a textbook project. It was

one crazy ride, and the process of writing a textbook unlocked the flow of words needed to write this dissertation. Thank you for that opportunity. Bill Abbott, Vanessa Correia, Sandie DeVries, Dylon McChesney, Jamie Sewell, Andy Stumpf, Chris Wass, and Sara Weaver were fellow collaborators, and I am thankful for their work and inspiration to keep writing stuff. Greg, let's do this again soon.

This dissertation grew out of a research area in the applicability of international law to cyberwarfare. That research area produced two conference presentations. I appreciate the responses and feedback from attendees and commentators, who helped assure me of the value of further developing the project. The members of my internal dissertation committee have all provided invaluable guidance. Matt Doucet, my supervisor, helped me keep intermediate goals in view rather than getting lost in the shadows lurking just beyond where I was working. Patricia Marino's initial support of the project and her ongoing affirmation that it was on a good philosophical track helped me keep going. Brian Orend, in addition to sparking the project, has been more than generous in his comments on earlier versions of the dissertation. I expected Brian to be the toughest critic of this work. He did not disappoint, but I was amazed by the encouraging manner in which he provided that criticism. Brian's commentary was on-point and inspiring. He corrected some misunderstandings, gave helpful suggestions for further development of ideas, identified ways to sharpen the focus of the dissertation, and provided reason to expand my book collection. The dissertation is much improved because of his feedback. I hope to have the opportunity to pay this debt forward.

Debbie Dietrich, Trish van Berkel, Angela Christelis, and Tawnessa Carter, the department's graduate administrators during my time at Waterloo, have all been key in navigating the University's processes and the glitches that always seem to arise.

I thank Mikhael Evstafiev for permission to include his photograph of Vedran Smailović in this dissertation.

The academy is not the only source of support I have had. I thank my circles of friends, and in particular those whom I have met in Waterloo, for practical help and encouragement. The part of the Christian church that gathers as the Waterloo parish of The Meeting House has graciously offered and provided generous assistance. I am also grateful for the medical and ac-

cessibility professionals who pointed to ways to manage the various personal challenges that become apparent only when leaving one's comfort zones.

There are technical debts to acknowledge as well. This dissertation was prepared on a 10-year-old MacBook Pro using Scrivener and MultiMarkdown. The illustrations were produced in OmniGraffle; the bibliography was managed using BibDesk. The work was typeset by XeLaTeX using the Baskerville 10, Barlow Condensed, and Bitstream Vera Sans Mono type families. It was scanned for originality by iThenticate under a licence provided by the University of Waterloo.

Finally, I return to the person I first named. I am indebted to Shelly for the encouragement and support she has given. Shelly has worked hard to sustain us both while I studied, taught, researched, and wrote, and has given me more loving grace than I deserve. Thank you. I love you.

Dedication

To Shelly, who led me into philosophy and patiently waited for me to crawl out, and to all who work for peace.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation for the project

In 2016 voter registration databases and email servers in the United States of America had their sensitive data stolen by Russian actors hoping to sow doubt about the integrity of that year's elections.[1] In 2015 two vehicle security researchers took control of a reporter's Jeep Cherokee, using a mobile Internet connection to disable the accelerator and brakes while the vehicle was on the road.[2] Utility companies have faced Internet-based attacks against their control systems, at least one of which caused a far-reaching electrical power outage.[3] While networked, computer-enabled technology provides many benefits for industry, business, society, and individuals, and even reduces some kinds of risks, these three examples show that the benefits come with a different set of risks. Some of those risks can result in trivial inconveniences, but the range of potential harm extends as far as the widespread loss of human life. This potential for wide-ranging harm makes these kinds of network-connected control systems and data servers attractive targets for

[1] Monique Garcia and Patrick M. O'Connell, "Illinois Elections Board 'Very Likely' Named in Mueller Indictment of Russian Hackers, Officials Say," *Chicago Tribune*, July 13, 2018, accessed February 25, 2019, `https://www.chicagotribune.com/news/local/politics/ct-met-illinois-elections-board-russia-indictment-20180713-story.html`.

[2] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, July 21, 2015, accessed January 11, 2018, `https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/`.

[3] Ellen Nakashima and Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *Washington Post*, January 19, 2008, A4.

interfering with the well-being of large numbers of people, particularly in the context of international tensions, conflicts, and wars.

It is no surprise that computing and network technology have become part of the military toolkit. The methods of waging war are continually evolving with the development of new technologies. Aircraft provided new abilities for reconnaissance and attacks, and made the skies a new battlespace. Nuclear weapons brought the possibility of bringing a nation to its knees—or obliterating its population entirely—with a small number of bombs. Computing and data systems are still newer warfaring technologies. These systems and their associated networks not only provide support for conventional military operations, but they can be legitimate military targets in their own right, and their vulnerability to data- and network-based attacks makes them particularly attractive. The effects of a well-targeted network attack can be extensive without incurring the material and human cost of a more conventional attack.[4] Systems and data or code that target other computing systems have become weapons in the new context of what has been called *cyberspace*, and war waged by or against such systems has been dubbed *cyberwarfare*.

But the practices of war are not unrestrained. Even though war intentionally breaches "the rules of law and morality applicable in peace-time—applicable to ordinary life," and that most of these breaches are broadly tolerated during (and only during) times of war, there is still some expectation that the extent of these breaches would be limited by some humane standard.[5] International humanitarian law, and in particular the international laws of armed conflict, are intended to serve this purpose.[6] As Henry Shue

[4]Committee on Offensive Information Warfare, Computer Science and Telecommunications Board, and National Research Council [USA], *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, ed. William A. Owens, Kenneth W. Dam, and Herbert S. Lin (Washington, DC: The National Academies Press, 2009), 27, `http://www.nap.edu/catalog/12651/technology-policy-law-and-ethics-regarding-us-acquisition-and-use-of-cyberattack-capabilities` (hereafter cited as Owens report).

[5]Henry Shue, "Laws of War," chap. 25 in *The Philosophy of International Law*, ed. Samantha Besson and John Tasioulas (Oxford, UK: Oxford University Press, 2010), 515.

[6]The terms *international humanitarian law* and *international laws of armed conflict* are often used interchangeably. However, international humanitarian law is intended to apply to all conflicts, while the international laws of armed conflict only apply to conflicts between states. Manfred Nowak, "Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment," chap. 16 in *The Oxford Handbook of International Law in Armed Conflict*, ed. Andrew

puts it,

> [t]he goal is to make war a rule-governed practice, with rules that limit its violations and its evils. It is not the purpose of these rules to end the practice [of war], or to maintain it. The practice is simply presupposed . . .
>
> . . . The purpose of the laws of war is to constrain the "shit" when the "shit" happens: when armies are assaulting and attacking, the laws of war specify firm limits.[7]

The international laws of armed conflict constrain how states can wage war against each other and impose imprecise limits on the harm that can lawfully be done to civilian persons, infrastructure, and objects in the context of an international armed conflict. These laws are expressed in various treaties, conventions, and protocols, and these instruments have been extended, amended, or created as means and methods of war develop. For example, the Geneva Conventions of 1906[8] and 1929[9] were superseded by the Geneva Conventions of 1949,[10] which were themselves extended by ad-

---

Clapham et al. (Oxford, UK: Oxford University Press, 2014), 407.

[7] Shue, "Laws of War," 515–6.

[8] International Committee of the Red Cross (ICRC), Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, July 6, 1906, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/C64C3E521F5CC28FC12563CD002D6737/FULLTEXT/IHL-GC-1906-EN.pdf (hereafter cited as Geneva Convention (1906)).

[9] International Committee of the Red Cross (ICRC), Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, July 27, 1929, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/09DFB7A98E19533AC12563CD002D6997/FULLTEXT/IHL-GC-1929-1-EN.pdf (hereafter cited as Geneva Convention (Wounded and Sick, 1929)); International Committee of the Red Cross (ICRC), Convention Relative to the Treatment of Prisoners of War, Geneva, July 27, 1929, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/0BDEDDD046FDEBA9C12563CD002D69B1/FULLTEXT/IHL-GC-1929-2-EN.pdf (hereafter cited as Geneva Convention (Prisoners of War, 1929)).

[10] International Committee of the Red Cross (ICRC), Geneva Conventions I–IV, August 12, 1949 (hereafter cited as GC I–IV (1949)).

ditional protocols in 1977[11] and 2005.[12] The first of these additional protocols incorporated specific protections for medical aircraft and stranded or incapacitated air crew who are no longer able to fight, and prohibited the intentional targeting of civilians in aerial attacks.[13] The second sets out the protections civilians and certain cultural objects have in cases of non-international conflict between organized armed groups within the territory of a state party to the protocol.[14] Further, AP I explicitly requires states party to the protocol to assess the permissibility, according to applicable international law, of using new means of warfare as they are developed.[15] This declaration means that it is both important and relevant to examine how international law controls (in ways analogous to older mans of war) the use of these new developments in computing, networking, and software technology. Implicit in that, but perhaps more readily overlooked, is the importance of exploring how the interpretation of international law may need further development or explication to address the kinds of harm those new weapons can produce. This dissertation project does both with respect to cyberwarfare.

[11] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Geneva, June 8, 1977, 1125 UNTS 3, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/D9E6B6264D7723C3C12563CD002D6CE4/FULLTEXT/AP-I-EN.pdf (hereafter cited as AP I); International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), Geneva, June 8, 1977, 1125 UNTS 609, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/AA0C5BCBAB5C4A85C12563CD002D6D09/FULLTEXT/AP-II-EN.pdf (hereafter cited as AP II).

[12] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem (Protocol III), Geneva, December 8, 2005, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/8BC1504B556D2F80C125710F002F4B28/FULLTEXT/AP-III-EN.pdf (hereafter cited as AP III).

[13] AP I, Art. 8, 24–31, 49, 57.

[14] AP II, Art. 1.

[15] AP I, Art. 36.

1.2 Goals and structure of the project

International laws of armed conflict apply to cyberwarfare

The first goal of the project is to argue, largely by analogy and equivalence, that there is not enough of a difference between cyberwarfare and conventional warfare to exempt cyberwarfare from the international laws of armed conflict. I develop this claim in Chapter 2 by responding to conjectures and problems presented by Randall Dipert in 2010.[16] Having established *that* these laws govern cyberwarfare, the rest of the project—examining *how* these laws can be applied to cyberwarfare—is justified. Along the way, I offer a description of what is meant by *cyberwarfare* and other related terms in the context of international humanitarian law and the international laws of armed conflict.

The *Tallinn Manual* represents international law fairly

In 2013 the first edition of the *Tallinn Manual*[17] was released. It has its origins in the aftermath of a crippling cyberattack made by Russian supporters against Estonia in 2007.[18] Its primary goal is to "bring[] some degree of clarity to the complex legal issues surrounding cyberoperations, with particular attention paid to those involving the *jus ad bellum* and the *jus in bello*,"[19] the two distinct legal contexts of the international laws of armed conflict. A revised edition followed in 2017 to "expand the Manual's scope to include the public international law governing cyber operations during peacetime."[20]

[16] Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 16, 2010): 384–410, https://doi.org/10.1080/15027570.2010.536404.

[17] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge, UK: Cambridge University Press, 2013), accessed September 18, 2015, http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (hereafter cited as *Tallinn 1.0*).

[18] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, accessed January 14, 2021, https://www.wired.com/2007/08/ff-estonia.

[19] *Tallinn 1.0*, 3–4.

[20] Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge, UK: Cambridge University Press, 2017), 1 (hereafter cited as *Tallinn 2.0*).

This revision includes expanded rules on state sovereignty, jurisdiction, control, and responsibility over cyberspace and provides updated commentary on some of the other rules set out in the earlier edition. Chapter 3 sets out the context and motivation for the development of the *Tallinn Manual*, which follows the model of earlier manuals concerning land, sea, and air warfare.

As a guide to understanding how both *jus ad bellum* and *jus in bello* apply to cyberwarfare, the *Tallinn Manual* invites comparison against the principles of just-war theory (from which the two phrases come) as well as the international laws of armed conflict. The international laws of armed conflict set out fewer *jus ad bellum* principles than just-war theory does for plausible reasons concerning the discernibility of intention and the equal sovereignty of states regardless of any imbalance in warfaring ability, and makes no specific reference to *jus post bellum*. Since the *Tallinn Manual* is meant to present international law and not the whole of just-war theory, it sets out rules that correspond only to the just-war principles upheld by international law. Chapter 4 applies the *Tallinn Manual*'s rules and commentary to different real and hypothetical examples, making reference to important sources of international law. I conclude that the *Tallinn Manual*, while incomplete with respect to just-war theory as a whole, is as faithful in its interpretation of *jus in bello* as manuals for other domains of warfare are, and breaks new ground in its extended discussion of just-cause criteria as part of *jus ad bellum*. It is, therefore, a useful and reliable distillation and exposition for both decision-makers and researchers[21] concerned with cyber operations in the international context.

The *Tallinn Manual* reveals the difficulty of assessing just cause

The *Tallinn Manual* presumes that no state actor desires to begin an international armed conflict. It is concerned with what happens after the first hostile action has been made against a state, either as a response to that action (*jus ad bellum*) or in the continuation of such a conflict (*jus in bello*). A primary concern with respect to *jus ad bellum* is to determine when the harm caused by an aggressive cyberoperation may provide just cause for (but not necessarily require) responding with a forceful act made in self-defence against another state; that is, when it reaches the level of an actionable "use of force"[22] under

[21] *Tallinn 2.0*, 2.

[22] United Nations, Charter of the United Nations, October 24, 1945, 1 UNTS XVI, Art. 2(4), accessed October 6, 2015, `http://www.refworld.org/docid/3ae6b3930.html` (hereafter

the terms of the United Nations Charter.

The *Tallinn Manual* sets out eight criteria to consider,[23] not as a checklist, but as considerations that, when they give rise to conflicting guidance, must all be addressed when determining whether just cause for a forceful response exists. I look closely at four of these in Chapter 5: first, the measurability of effects and the severity of harm produced by an initial aggressive cyberoperation, and then the temporal immediacy and causal directness of those effects. I show that causal directness and temporal immediacy are necessarily separate considerations that, taken individually, can provide differing guidance with respect to having just cause for responding to a cyberattack with a use of force. I also show that aggressive cyberoperations can result in some harms that are not readily comparable to those produced by conventional attacks, but go beyond the level of an inconvenience. The guidance given in the *Tallinn Manual* is of limited value in those intermediate cases. To address these problems I present, then expand, a conceptual temporal schema first set out by William Owens and others[24] for analyzing the emergence and severity of any harm produced by an aggressive cyberoperation, and introduce means of classifying cyberattacks and responses in terms of their actual or intended effects, demonstrating the value of those frameworks through examples.

International law mandates greater protections for data objects

The most significant goal of this project is to argue that states already have obligations to protect data relevant to the safeguarding of human rights. The international laws of armed conflict, international humanitarian law, and international human rights law all set out obligations for parties involved in armed conflict. Human rights law is the one that applies in all contexts. International humanitarian law applies to all armed conflict (and so to non-state actors), while the international laws of armed conflict apply only to conflicts between states.[25] Some of those obligations require positive actions

cited as UN Charter).

[23] *Tallinn 2.0*, Rule 69, comment 9.

[24] Owens report, 89–91.

[25] Nowak, "Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment," 407.

to safeguard human rights, and in particular, the rights to an identity and to not be arbitrarily deprived of life, liberty, or security of the person.[26]

One positive step toward safeguarding these rights is to honour the obligation to record every child's birth.[27] Preserving rights requires preserving the record of the person's existence, which suggests that certain civil records must be protected from harm during armed conflict, whether internal or international. This has always been a problem, since the storage of multiple copies of paper records is inefficient, but paper documents are also readily destroyed. Storing these records in digital form requiring network access to data servers makes data redundancy less expensive, but also leaves the records susceptible to a cyberattack, not just a physical attack. Chapter 6 argues that the emergence of cyberwarfare draws attention to both the vulnerability and importance of that information, and gives support to the opinion of some experts in international law that digital representations of civil records and cultural objects enjoy such protection.

This gap in protection comes into focus through studying the human rights violations that took place in the Kosovo conflict of 1998–99. These violations came through the destruction of civil records, including identity documents and property records. Other examples demonstrate how the loss of these kinds of records affect not only the lives of persons but also the cultural heritage of humanity. I conclude that the *Tallinn Manual* understates the strength of the argument that these obligations already exist and are not new impositions on states party to the relevant human rights treaties. While international law already mandates this kind of protected data-keeping, more work must go into actually doing it.

---

[26] United Nations General Assembly, Universal Declaration of Human Rights, December 10, 1948, A/RES/217(III), Art. 3, accessed January 5, 2021, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf (hereafter cited as Universal Declaration); United Nations General Assembly, International Covenant on Civil and Political Rights, December 16, 1966, 999 UNTS 171, Art. 6, 9, accessed February 12, 2019, https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (hereafter cited as ICCPR).

[27] United Nations General Assembly, Convention on the Rights of the Child, November 20, 1989, 1577 UNTS 3, Art. 7, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/B92BDC3CAE1B142DC12563CD002D6E8C/FULLTEXT/IHL-86-EN.pdf (hereafter cited as Rights of the Child).

Important work in this area remains

The final chapter demonstrates the relevance of this work in larger contexts opened up by the development of computing and communications technology. Specific topics for further study include the need to maintain a conceptual separation of the information content of data from the transportation, storage, and processing systems of cyberspace; providing different levels of protection to data based on the purpose the data serves; the exercise of human rights in cyberspace; how state sovereignty can be violated by even moderate cyberattacks; the responsibility of states for non-state actors; and cyberspace in outer space. All of these are connected to cyberoperations, human rights, and the preservation of international peace.

The general public can grasp the importance of the work

Concerns such as these need to be accessible to the general public. Thus one of the aims of this research project (and not just the dissertation) is to offer to the general public my justification for doing this work.

Human rights matter for everyone. The way I chose to get that point across in a public forum was to show how difficult it can be to defend your own rights if there is no documentation to support them. Appendix B contains the main finding of Chapter 6 distilled down to a three-minute monologue presented at the University of Waterloo's *3-Minute Thesis* competition in 2018.

Chapter 2

Cyberwarfare: the new threat on the block

2.1 The desire to control cyberwarfare

Sometimes the initial response to a new means of warfare is along the line of "This changes everything!" This reaction greeted the use of nuclear and chemical weapons, and there are some who believe the same about cyberwarfare. It is tempting to conclude that the international laws of armed conflict are not relevant to this new reality of war. International law is generally prohibitive, not permissive, so actions that may cause harm to another state but are not explicitly proscribed by treaty, law, or convention are presumptively lawful.[1] Thus any act of cyberagression is permissible, and no international law governs cyberwar. One presentation of this view has been articulated by Randall Dipert.[2] Dipert develops an argument to justify the claim that

[1] Permanent Court of International Justice (PCIJ), *The Case of the ss* Lotus *(France v. Turkey)*, 1927 PCIJ (ser. A) 10, September 7, 1927, ¶¶44–7, accessed November 24, 2020, `http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm` (hereafter cited as *Lotus*), cited in *Tallinn 2.0*, Rule 69, comment 9(h).

[2] Dipert, "The Ethics of Cyberwarfare." Further developments have shown that the international community has not bought into the argument Dipert presents, and Dipert may no longer be a defender of this view. Even so, the argument Dipert offers is an important one, for the reasoning is plausible, and it raises important questions about the applicability of international law to cyberwarfare. Responding to the argument requires a careful analysis of warfare in general, cyberwarfare in particular, and the international laws of armed conflict.

"most legal frameworks do not clearly apply to many instances of cyberwarfare, and cyberwarfare involves aspects of damage or harm that are typically not addressed by law,"[3] including the international laws of armed conflict. With this statement, Dipert kickstarts the dialogue to ascertain the extent to which existing international law may apply to cyberwarfare—if it does at all.

The number of proposals for some kind of international treaty to govern the use of cyberspace lends a small degree of indirect support to this view. If international law does not apply, then parties negotiating in good faith might negotiate a new treaty—and new international law (at least among parties)—that will apply. Yet only a few limited treaties have been negotiated concerning cyberspace, and only two were concluded before Dipert's article appeared. The first is the 2001 Budapest Convention on Cybercrime.[4] However, that treaty does not address cyber*warfare* in the context of international armed conflict, only the treatment of criminal activity by non-state actors.[5] The second is the 2009 agreement among Russia, China, Kazakhstan, Uzbekistan, Kyrgyzstan, and Tajikistan,[6] but this agreement goes beyond cyberspace to any means of conveying information and to the control of information itself ("the global information space"[7]) regardless of the medium.[8] Thus it is not strictly a cyberspace treaty. Subsequent attempts to arrive at a comprehensive treaty concerning either cyberspace as a battlespace (analogous to the Outer Space Treaty[9]) or cyberoperations as a

[3]Dipert, "The Ethics of Cyberwarfare," 395.

[4]Council of Europe, Convention on Cybercrime, November 23, 2001, ETS 185, accessed November 24, 2020, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[5]Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86, no. 2 (March 2010): 524n5, https://doi.org/10.1111/j.1468-2346.2010.00894.x.

[6]Shanghai Cooperation Organization, Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, June 16, 2009, unofficial translation, accessed November 25, 2020, http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf (hereafter cited as Shanghai Cooperation Agreement); Kristen E. Eichensehr, "International Agreements—and Disagreements—on Cybersecurity," *Just Security*, October 24, 2014, accessed November 23, 2020, https://www.justsecurity.org/16706/international-agreements-and-disagreements-on-cybersecurity/.

[7]Shanghai Cooperation Agreement, preamble.

[8]Shanghai Cooperation Agreement, Annex 2, ¶5.

[9]United Nations, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, January 27,

means of war (analogous to the Chemical Weapons Convention[10]) have also failed, most recently during negotiations at the United Nations in 2017.[11] Even so, these attempts do not establish the claim that international law does not apply to cyberwar, only that as yet there is no treaty or convention explicitly governing cyberwar.

I discern two key points that directly support the argument Dipert offers: the novelty and nature of cyberweapons. In response, I argue that neither the novelty of cyberwarfare nor the lack of explicit mention of cyberwarfare in existing international law require a wholesale revision of the international laws of armed conflict. The limitations on methods and means of warfare[12] and the anticipation of new kinds of weapons set out in the 1977 Additional Protocols[13]—long after the development of nuclear and chemical weapons—suggest this. I will also show that these limitations have support in earlier statements of international law. I further argue that there is no relevantly significant difference between cyberwarfare and conventional warfare, so international law applies to cyberwarfare in an analogous way to other means of warfare. If my argument in this chapter succeeds, then it follows that cyber means of war can not only be used lawfully, but also that existing international law is adequate to address in general terms the permissibility and limitations of cyberwarfare. I do this by responding to each of the main questions Dipert raises about cyberwarfare.

1967, 610 UNTS 205, accessed November 28, 2019, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html (hereafter cited as Outer Space Treaty).

[10] United Nations, Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Paris, January 13, 1993, 1974 UNTS 45, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/9D3CCA7B40638EF5C12563F6005F63C5/FULLTEXT/IHL-87-EN.pdf (hereafter cited as Chemical Weapons Convention); Ido Kilovaty and Itamar Mann, "Towards a Cyber-Security Treaty," *Just Security*, August 3, 2016, accessed November 23, 2020, https://www.justsecurity.org/32268/cyber-security-treaty/.

[11] Michael Schmitt and Liis Vihul, "International Cyberlaw Politicized: UN GGE's Failure to Advance Cyber Norms," *Just Security*, June 30, 2017, accessed November 23, 2020, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[12] AP I, Art. 35.

[13] AP II, Art. 36.

2.2 Bounding *cyberwarfare*

The word *cyberattack* has become commonplace in news headlines, and the corresponding articles often place responsibility on an international group of hackers (in the sense of persons interfering with systems rather than seeking a deep understanding of them) or agents of another state's government. These attacks are often used to copy sensitive information and use it for a harmful purpose. While these acts do some harm to the affected parties, there are some who believe that these kinds of aggressive cyberoperations cannot be acts of war because their effects are either too small or too localized to be a significant threat to the state from which the data were copied.[14] But what if the effects of a cyberattack do cause significant physical harm? What if the cyberattack is against a privately-owned civilian data centre? Are those cyberattacks act of cyberwar? If so, what responses to those cyberattacks might a state lawfully make?

There are several descriptions of what might fall under the concept of *cyberwarfare*. Jeffrey Carr pithily describes *cyberwarfare* as "the art and science of fighting without fighting; of defeating an opponent without spilling their blood."[15] Carr's description misses significant aspects of warfare. The lack of bloodshed is not unique to cyberwarfare. Not all acts of war are intended to kill or injure people, but to disrupt critical infrastructure such as transportation, dams, and power generating stations. Further, cyberwarfare is not inherently bloodless. Some aggressive cyberoperations—particularly those that are designed to cause critical infrastructure such as hydroelectric generating stations to fail—can produce human injuries and deaths in the target state. Dipert's analysis avoids Carr's oversight. Dipert begins with what he calls a *cyberharm*: a disruption of the normal functioning of some system ("a person, a machine, software or an economy"[16]) brought about by means of data itself or a data communication system. He also recognizes there must be a measure of intent to inhibit some command or information

[14] International Committee of the Red Cross (ICRC), "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts," in *31st International Conference of the Red Cross and Red Crescent*, doc. 31IC/11/5.1.2, report (Geneva, CH: International Committee of the Red Cross, November 28–December 1, 2011), 37, accessed November 27, 2020 (hereafter cited as Challenges of Contemporary Armed Conflict (2011)).

[15] Jeffrey Carr, *Inside Cyber Warfare*, 2nd ed. (Sebastopol, CA: O'Reilly Media, 2011), 7.

[16] Dipert, "The Ethics of Cyberwarfare," 397.

system from working as expected for the cyberharm to be considered a *cyberattack*. However, intent by itself is not sufficient to call these cyberattacks acts of *cyberwar*. That requires the involvement of state-controlled political or military agents.[17] For the purposes of his argument, Dipert considers only "cyberattacks (intentional cyberharms) that are instigated or controlled by political institutions (or their military services) on other political organizations or military services." If the belligerents are recognized states, and "the attacks between political entities are sufficiently 'widespread' we might then speak of a cyber*war*." But then he "stipulate[s] that war in its usual sense involves the intentional use of deadly force on human beings," concluding that "[a] cyberwar might not then literally be a war in this stricter sense, unless death or severe injury of human beings was the further intended result."[18]

A current American military publication defines *offensive cyberspace operations* as "[c]yberspace operations intended to project power by the appli-

[17]Non-state parties such as corporations, activist groups, and criminal organizations do not have authority to declare or initiate war in anything more than a figurative sense. UN Charter, Art. 51; Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, ed. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy and National Research Council [USA] (Washington, DC: National Research Council [USA], The National Academies Press, June 10–11, 2010), 171, `http://www.nap.edu/catalog/12997/proceedings-of-a-workshop-on-deterring-cyberattacks-informing-strategies-and` (hereafter cited as Cyber Operations in International Law). Cyberattacks conducted by or against these parties are, with rare exceptions, governed by international and domestic criminal law, not laws of armed conflict, and as such should be considered acts of *cybercrime*, not *cyberwar*. Charles J. Dunlap Jr., "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar," chap. 13 in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (Boca Raton, FL: Taylor & Francis, 2013), 214–15, `https://doi.org/10.1201/b15253-17`; Randall R. Dipert, "The Essential Features of an Ontology for Cyberwarfare," chap. 5 in Yannakogeorgos and Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 35. This requirement does not address acts of non-state terrorism, which are often treated as acts of war in political rhetoric. However, terrorist groups are not recognized by the international community as having the authority to declare war against a state. On this account, then, terrorism is an international criminal matter. I do not intend to defend or affirm this stance. I only note that despite the extensive harms caused by terrorist activity, international law excludes terrorism from the discussion at hand.

[18]Dipert, "The Ethics of Cyberwarfare," 398. Emphasis in original.

cation of force in or through cyberspace."[19] This falls in line with Dipert's politically-motivated cyberattacks. However, not all applications of force by cyberspace operations (*cyberoperations*) are acts of war.[20] Dipert acknowledges this, requiring that thresholds of scale ("sufficiently 'widespread' ") and intended effect ("death or severe injury of human beings") be met before an aggressive cyberoperation can be called an act of war. Further, the international community's understanding of an act of war is somewhat broader than what Dipert stipulates. For example, the United Nations General Assembly has resolved that "[b]ombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State''[21] should be construed as an act of aggression in United Nations Security Council deliberations. Nonetheless, Dipert's stipulation is useful for the purpose of argument, for if human injury or death results, the threshold of being an aggressive action is clearly met. I show the significance of these thresholds in Chapter 5.

The international laws of armed conflict cannot precisely define *cyberwarfare* because they do not define *acts of war*. The terms *use of force* and *armed attack*, both of which help the international community determine what might be considered acts of war, are themselves open-textured. Correctly determining what falls under each of them depends upon the quality of information used to assess multiple imprecise criteria. Further, even though there is no explicit mention of cyberwarfare in current international law, there are guidelines and precedents to consider when determining what intentional acts of international cyberharm could meet existing criteria for being declared an armed attack. The *Tallinn Manual*,[22] developed for the Cooperative Cyber Defence Centre of Excellence (CCDCOE) located in Tallinn, Estonia, presents some of these considerations. The *Tallinn Manual* also does not de-

[19] Department of Defense [USA], *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (As Amended through 15 June 2015)* (June 15, 2015), 174, accessed October 23, 2015, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[20] Cyber Operations in International Law, 163.

[21] United Nations General Assembly, "Definition of Aggression," Resolution 3314 (XXIX), December 14, 1974, Art. 3(b), accessed January 30, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX). The resolutions of the General Assembly do not establish international law until the Security Council adopts them in a separate vote, but they are indicative of the direction the supporters of the resolution believe international law should go.

[22] *Tallinn 1.0*; now superseded by *Tallinn 2.0*.

fine what an *act of war* is, so it, too, cannot define *cyberwarfare*. Instead, it considers multiple imprecise, but principled, criteria to determine whether a particular cyberoperation meets the thresholds of being a use of force and an armed attack. Roughly, this requires that the effects of the cyberoperation are at least equivalent to what would be caused by an armed attack conducted by conventional means such as bombs, missiles, or troops. Given the lack of a clear definition of *cyberwarfare*, and the standards by which an aggressive act is judged to be an act of war, a robust but imprecise description of *cyberwarfare* seems appropriate. For the purposes of this project, then, the term *cyberwarfare* is constrained to describe military actions of states against other states as a means of attaining political goals, where such actions target or involve the disruption, degradation, or destruction of some computing device, its programming, its data, or its communication systems by means of an operation conducted in cyberspace, and where the effects of such actions rise to the level of harm equivalent to that of an armed attack, and/or are conducted in the course of an ongoing international armed conflict. This description accommodates most of Dipert's analysis, but also acknowledges the difficulty (if not impossibility) of establishing a one-size-fits-all set of rules for calling a cyberattack an act of war. The open texture of this description is not a fatal flaw, but is a desirable characteristic shared with other concepts in legal contexts: edge cases require careful, nuanced deliberation to determine whether the concept reasonably applies.

2.3 Some terminology and concepts

The international laws of armed conflict have their own terms of art for specific concepts. Four are particularly significant: *necessity*, *proportionality*, *means of warfare*, and *methods of warfare*. The first two have their roots in just-war theory; these terms are connected to the conditions required for a state to enter a war lawfully (*jus ad bellum*, set out in Table 2.1) and the obligations imposed upon a state's military forces in order to conduct that armed conflict lawfully (*jus in bello*, set out in Table 2.2). Just-war theory and some international laws (but not the international laws of armed conflict yet) are evolving to incorporate the moral requirements to end a war in a way that

	***Jus ad bellum* conditions**[a]
just cause	self-defence, protection of innocents from aggression
right intention[b]	objective is to secure the just cause and nothing more
public declaration	citizens of declaring state and governments of enemy states are informed of the declaration
appropriate authority	declaration made in accordance with declaring state's constitution and/or legislation
last resort	all other plausible means of resisting aggression have failed
probability of success[b]	engaging in war will not be a futile exercise undertaken in exasperation or desperation
proportionality	expected benefit to all parties supports the anticipated universal cost borne by all parties

Table 2.1: *Jus ad bellum* conditions of just-war theory. All of these conditions must be satisfied before an initial act of war is permissible under just-war theory.

[a] Summarized from Brian D. Orend, "War," in *Stanford Encyclopedia of Philosophy*, Spring 2016, ed. Edward N. Zalta (July 28, 2005), §2.1, accessed October 27, 2015, `http://plato.stanford.edu/archives/fall2008/entries/war/`.

[b] Not incorporated within the international laws of armed conflict.

re-establishes "minimally just societ[ies],"[23] ideally with no further cause to engage in an international armed conflict (*jus post bellum*, described in Table 2.3). Some of these concepts will show up again in Chapters 4 and 6.

Necessity

Necessity is not a term that appears in the *jus ad bellum* or *jus in bello* principles of just-war theory. Nonetheless, it is a term that shows up in the discussion

[23] Brian D. Orend, "War," in *Stanford Encyclopedia of Philosophy*, Spring 2016, ed. Edward N. Zalta (July 28, 2005), §2.3, accessed October 27, 2015, `http://plato.stanford.edu/archives/fall2008/entries/war/`.

	***Jus in bello* obligations**[a]
no prohibited weapons	in accordance with "public conscience"[b] and international law
discrimination	of combatants and military facilities from civilians and purely civilian facilities
proportionality	of degree of force employed to the effort required for achieving the anticipated military objective
no means evil in themselves	precludes the use of indiscriminate, dehumanizing, or treacherous activities
no reprisals	against enemy states' violations of these criteria that violate these criteria themselves
benevolent quarantine	for enemy personnel no longer actively engaged in the conflict, such as prisoners of war
respect	for the rights of the warring state's own citizens

Table 2.2: *Jus in bello* obligations of just-war theory. The first five of these obligations are constraints on the use of force. For any use of force in an armed conflict to be permissible, it must fall within the parameters established by these constraints. The last two obligations preserve the rights of non-combatants.

[a] Summarized from Brian D. Orend, "War," in *Stanford Encyclopedia of Philosophy*, Spring 2016, ed. Edward N. Zalta (July 28, 2005), §2.2, accessed October 27, 2015, `http://plato.stanford.edu/archives/fall2008/entries/war/`.

[b] Hague Peace Conferences, Convention (IV) Respectting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, October 18, 1907, preamble, accessed January 3, 2021, `https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/4D47F92DF3966A7EC12563CD002D6788/FULLTEXT/IHL-19-EN.pdf` (hereafter cited as HC IV (1907)).

***Jus post bellum* requirements**[a]	
proportionality	negotiated settlement is reasonable and does not impose excessive punishment on the defeated party; analogous to proportionality in both *jus ad bellum* and *jus in bello*
public proclamation	informs civilians, combatants, allied states, and the rest of the international community that the armed conflict is ended; corresponds to public declaration in *jus ad bellum*
vindication of rights	secures the "basic rights whose violation"[b] served as just cause for the conflict under *jus ad bellum*
discrimination	of leaders, combatants, and civilians when imposing punishment; analogous to discrimination in *jus in bello*
just punishment of leaders	for any war crimes and rights violations committed or encouraged
just punishment of combatants	for any war crimes and rights violations committed, regardless of which side of the conflict the combatant was on
restitution	for harm done by defeated state, while leaving the means "to begin its own reconstruction";[b] this may need to be symbolic
rehabilitation	of institutions required to support a minimally just society and a legitimate government

Table 2.3: *Jus post bellum* requirements of just-war theory. These emerging requirements are intended to ensure that the defeated states will establish minimally just societies under legitimate governments, while leaving no need to resort to armed conflict under *jus ad bellum*.

[a] Summarized from Brian D. Orend, "War," in *Stanford Encyclopedia of Philosophy*, Spring 2016, ed. Edward N. Zalta (July 28, 2005), §2.3, accessed October 27, 2015, `http://plato.stanford.edu/archives/fall2008/entries/war/`.

[b] Orend, "War," §2.3.

of what actions may be permissible under international law in response to different scenarios. One particularly fraught instance of the term appears to permit a state to absolve itself of responsibility for taking an action that violates an international obligation by pleading necessity in situations where the offence

> (a) is the only way for a State to safeguard an essential interest against a grave and imminent peril; and
> (b) does not seriously impair an essential interest of the State or States toward which the obligation exists, or of the international community as a whole.[24]

However, there are elements of existing international law that preclude making such a plea, and as Marco Sassòli notes, "international humanitarian law is a law that was made for armed conflicts, which are by definition emergency situations. It therefore explicitly excludes the defence claim of necessity, except where explicitly stated otherwise in some of its rules."[25] Pleading self-defence also preclude judgements of wrongfulness "if the act constitutes a lawful measure of self-defence undertaken in conformity with the Charter of the United Nations,"[26] which is settled international law. For the purposes of this project, then, *necessity* refers to its usage in the limited context of the international laws of armed conflict.

In the *jus ad bellum* context of international law, *necessity* presumes that there is a legitimate state authority to publicly declare a war for just cause.

[24] United Nations International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts," supplement No. 10 (A/56/10), ch. IV.E.1, November 2001, Art. 25(1), accessed December 11, 2020, `https://legal.un.org/ilc/reports/2001/english/chp4.pdf` (hereafter cited as Responsibility of States). These articles are not yet part of a convention or treaty, though many state and international organizations, including courts, make reference to them as customary international law. United Nations, "Tackling State Responsibility, Diplomatic Protection Drafts, Sixth Committee Delegates Argue over Elaborating Texts into Conventions," meetings coverage, Sixth Committee, Seventy-Fourth Session, 13th & 14th Meetings (AM & PM), GA/L/3598, October 15, 2019, accessed December 11, 2020, `https://www.un.org/press/en/2019/gal3598.doc.htm`.

[25] Marco Sassòli, "State Responsibility for Violations of International Humanitarian Law," *Revue Internationale de la Croix Rouge* 84, no. 846 (June 2002): 415–6, accessed December 11, 2020, `https://www.icrc.org/en/doc/assets/files/other/401_434_sassoli.pdf`, with further references.

[26] Responsibility of States, Art. 21.

Making such a declaration further presumes that all other available means for resolving the dispute have been exhausted. (International law acknowledges the difficulty of judging right intention, and so does not incorporate this just-war criterion. Nevertheless, starting a war certainly indicates that state authorities believe they have, at the very least, plausible deniability against charges of acting without a right intention.) Restricting the declaration of war to appropriate state authorities and requiring the declaration to be communicated to the enemy state or states limits the right to engage in armed conflict to states, thereby excluding non-state organizations from lawful participation in their own right. Moreover, only states (and not non-state actors such as *Daesh*, Google, Alberta, or drugs) can be on the receiving end of the declaration. The state authorities that have the right of declaring war are determined by each state in accordance with its constitution and other relevant legislation, provided that the government is recognized by the international community. So-called *failed states*, that is, states lacking a minimally functioning government, do not have an internal authority that can declare war or receive a declaration of war on behalf of the state, and so do not have a right to participate lawfully in an international armed conflict.[27] With respect to just cause, the international laws of armed conflict recognize only two that might support the necessity of declaring war: self-

[27] An ICRC preparatory document sets out the reasoning:

> Under international law, a State is an entity that has a defined territory and a permanent population, under the control of its own government, and that engages in, or has the capacity to engage in, formal relations with other such entities.
>
> The disintegration of State structures seems to occur when the third constitutive element of statehood, a government in effective control, fades away. [. . .]
>
> A situation of this type . . . involves the implosion of national institutions, authority, law and order, in short, the body politic as a whole. It also implies the breakdown of a set of values on which the State's legitimacy is based . . . The State itself does not physically disappear, but gradually loses the capacity to carry out the normal functions of government.

International Committee of the Red Cross (ICRC), "ICRC, Disintegration of State Structures," *How Does Law Protect in War? Online Casebook*, 1998, §1, accessed December 15, 2020, `https://casebook.icrc.org/case-study/icrc-disintegration-state-structures#part_ii_2`. A state's functional disintegration does not absolve factions within the state of the obligation to observe international humanitarian law.

defence (as determined by the victim state, but also subject to a standard of reasonableness)[28] and whatever the United Nations Security Council declares (presumably after reasoned deliberation).[29]

Within the *jus in bello* context of international law, *necessity* takes on a different sense, that of *military necessity* with respect to particular objectives.[30] This sense of *necessity* has no corresponding concept in the *jus in bello* obligations of just-war theory. However, having established some claim that the use of force has become permissible under *jus ad bellum*, any uses of force are subject to the restrictions set out under *jus in bello* in order to respect "the protection of the civilian population and civilian objects" and to prevent "unnecessary suffering of combatants" as a result of any use of force.[31] The principle of *proportionality* is of particular importance here.

Proportionality

Proportionality is a feature of both the *jus ad bellum* conditions and the *jus in bello* obligations, but with different senses within each context. With respect to entering into an armed conflict, *proportionality* requires that the benefits expected to accrue globally (and not just across all parties involved in the conflict or an individual state) will be greater than the accumulated harms inflicted globally (and not just upon all parties in the conflict or an individual state). As with *necessity*, this assessment is fraught. First, it is difficult to assess all of the effects because of the human tendency to discount unforeseen or distant consequences. Second, the assessment is easily biased toward the narrow interests of each individual state involved in the conflict.[32] (The *probability of success* criterion of just-war theory is connected to this assessment, since a brutally honest and comprehensive assessment resulting in a non-positive total signals a low probability of achieving the intended outcome. However, this is not a criterion of international law because it de-

[28] UN Charter, Art. 51.

[29] UN Charter, Art. 42.

[30] *Tallinn 2.0*, Rule 72, comment 1.

[31] International Court of Justice (ICJ), *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 1996 ICJ 226, July 8, 1996, ¶78, accessed November 24, 2015, `http://www.icj-cij.org/docket/files/95/7495.pdf` (hereafter cited as *Nuclear Weapons Advisory Opinion*).

[32] Orend, "War," §2.1.

prives militarily weaker and/or economically poorer states of their sovereign right to enter into armed conflict in self-defence.[33])

Once an armed conflict is under way, each military action must be assessed with respect to the degree of force required to achieve each particular military objective. Having determined that there is a military necessity for taking a particular action, the *jus in bello* obligation of *proportionality* prohibits using excessive force (that is, causing more than the justifiable expected damage to civilian persons and objects) to achieve a military advantage.[34] This is connected to the *jus in bello* obligation of *discrimination*, which specifies that only combatants and military facilities are lawful targets.[35] Any use of force that cannot discriminate between combatants and non-combatants or between military and civilian facilities is likely to be disproportionate with respect to the degree of force that may be permissible under international law because the effects go beyond what is militarily necessary to achieve the particular objective.

Means and *methods of warfare*

Means of warfare "generally refer to the weapons being used" in an armed conflict, and *methods of warfare* "generally refers to the way in which such weapons are used."[36] The methods and means of warfare are subject to the *jus in bello* obligations of international law. Thus some means of warfare are permissible when used against enemy combatants, but indiscriminate use of those means, such as disregarding protection for civilians, are prohibited methods of warfare.[37] Other means and methods of warfare are prohibited under international law because they cannot be used in a way that recognizes the principle of distinction (for example, chemical or biological weapons).[38]

---

[33] Orend, "War," §2.1.

[34] AP I, Art. 51(5)(b), referenced in *Tallinn 2.0*, Rule 113, comment 1.

[35] AP I, Art. 51, 52.

[36] Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann, eds., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva, CH: Martinus Nijhoff, 1987), §1957, accessed January 6, 2016, `http://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf` (hereafter cited as *Commentary on the Additional Protocols*). Sometimes the word *conflict* is used in place of *warfare*.

[37] *Commentary on the Additional Protocols*, §1402.

[38] International Committee of the Red Cross (ICRC), *Rules*, vol. 1 of *Customary International Humanitarian Law*, ed. Jean-Marie Henckaerts and Louise Doswald-Beck (Cambridge, UK:

There are also means and methods deemed to be *evil in themselves* (*mala in se*) because they result in excessive suffering beyond what is required to render an enemy combatant unable to participate further (such as land mines or blinding weapons),[39] or are gross violations of non-combatant or fundamental human rights (actions like perfidy, rape, starvation, or enslavement).[40]

2.4 Why international law might not apply

Dipert poses five questions to challenge the uncritical assumption that cyberattacks (military-political intentional cyberharms) and responses to such attacks are permissible under international law:

1. Is a cyberattack ever morally justified in response to an enemy *conventional* attack?
2. Is a cyberattack ever morally justified in response to an enemy *cyberattack*?
3. Is a *conventional* attack ever morally justified by an enemy *cyberattack*?
4. Is a cyberattack ever morally justified in cases where the enemy has launched neither a cyber- nor a conventional attack? (With United Nations sanction, preemptively, preventively, or for some other reason.)
5. Once a war (cyber- or conventional) has begun what kinds of cyberattacks are morally justified?[41]

Dipert suggests that the answer to justifying a cyberattack in response to cyber- or conventional attacks (his first two questions) is a provisional *yes*, subject to being able to justify using cyberattacks at all (his fifth question).[42] He calls the third and forth of these questions—responding to a cyberattack by conventional means, and making an initial cyberattack—"the hard

Cambridge University Press, 2005), Rules 1, 7, accessed April 20, 2018, `https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf`.

[39] *Nuclear Weapons Advisory Opinion*, ¶78.

[40] International Committee of the Red Cross (ICRC), *Rules*, Rules 53, 58–65, 88–99, 103.

[41] Dipert, "The Ethics of Cyberwarfare," 392–393

[42] Dipert, 392.

cases"[43] because they force us to examine just what a cyberattack is and whether it is significantly different from other kinds of attacks when considered under international law.

Dipert's first "hard case" concerning justifiable responses to cyberattacks depends on reliably identifying the attacker (the "Attribution Problem").[44] This can be particularly difficult to do in a timely fashion, for sources of cyberattacks are readily obfuscated.[45] The attribution problem identifies an epistemic requirement for launching a counterstrike to a cyberattack, and Dipert rightly observes that this requirement in a cyber context is similar to what is required before responding to a conventional attack.[46] A strike made by conventional means leaves clues about its origin: the bordering state in the case of troops, the flight path for aircraft and projectiles, the identification on any pieces of ordnance that remain after impact. These are difficult to disguise, so identifying the attacking party is relatively simple. But the origin of a cyberattack is often more difficult to determine, and unravelling the multiple possible layers of obfuscation through encryption and forgery of identifying information takes time. Nonetheless, this complexity does not change the epistemic requirement to identify the source of the attack before launching a lawful counterstrike. As a result, Dipert's question about responding to a cyberattack by conventional means really asks whether a cyberattack that causes only non-lethal and temporary harm to a state is just cause for a conventional war, even taking into account the death and destruction that would follow.[47] If a cyberattack turns out to be similar to conventional attacks that are just cause for a response, then the answer to this question is *yes*; if not, then the answer is *no* unless there is some other way to justify an armed response.

Dipert's second "hard case" is about the justification of an initial cyberattack. This problem is similar to the problem of justifying a preemptive strike in a conventional context, though he anticipates that any preemptive cyberattack would be "free of the usual death and destruction of traditional

[43] Dipert, "The Ethics of Cyberwarfare," 393.

[44] Dipert, 393.

[45] Ned Moran, "A Cyber Early Warning Model," chap. 12 in Carr, *Inside Cyber Warfare*, 179.

[46] Dipert, "The Ethics of Cyberwarfare," 393.

[47] Dipert, 394.

forms of warfare."[48] However, Dipert claims that on a literal reading of Articles 2(4) and 51 of the United Nations Charter,[49] the definitionally vague notion of *armed attack* "seems . . . to designate soldiers using 'arms,' roughly as artifacts for inflicting injury, death, or causing physical destruction of objects."[50] But a cyberattack executed by "an information-theoretic entity" such as (but not limited to) a general-purpose computer is not carried out using such artifacts, and so is not addressed under international law.[51] Further, he claims that cyberwarfare is too novel for ethical and policy discussions to resolve how cyberweapons may be used in international conflict,[52] so international law cannot yet be written to address cyberwarfare. Thus the international law of armed conflict is not fit to address his notion of *cyberwarfare*. The answer to this question depends on the similarity of cyberattacks to other attacks and to what extent international law has already accounted for new means of war. If cyberattacks are in some way equivalent to conventional attacks and so are covered under existing international law, then this question has the same answer as one would give to the question of preemptive strikes in general. If they are something different, then some of Dipert's conclusion has merit. This would leave open the possibility that preemptive cyberattacks may be justifiable on some ground other than current international law.

I address two parts of Dipert's argument for excluding cyberwarfare from the reach of international law: his concerns about the nature of cyberwarfare, which affects the answer to both of these hard cases, and the novelty of cyberwarfare, which affects the answer to the second hard case.

2.5 Novel means, similar effects

Dipert wants to distinguish between cyberattacks from traditional kinetic attacks for two reasons. First, cyberattacks are a novel development in warfare. Second, cyberattacks appear to be different in some significant way from kinetic attacks. Dipert draws on a National Research Council [USA] report (the

[48] Dipert, 393.
[49] UN Charter.
[50] Dipert, "The Ethics of Cyberwarfare," 395.
[51] Dipert, 395–396.
[52] Dipert, 385.

Owens report) acknowledging that cyberattacks are different from kinetic attacks in important ways and identifying the need for some careful thinking about the legal and ethical concerns around cyberwarfare.[53] However, another chapter of the Owens report also notes that there are other non-cyber weapons in the warfarer's arsenal that are not kinetic in the sense that thermochemical bombs and projectiles are, yet are considered "weapons of mass destruction (for example, nuclear, chemical or biological weapons)."[54] These weapons were also once novel means of war, and their development resulted in a great deal of ethical, legal, and political work concerning their justifiable use or prohibition in war. The Biological Weapons Convention of 1972[55] and the Chemical Weapons Convention of 1993[56] affirm and extend the principles expressed in the 1925 Geneva Protocol prohibiting bacteriological weapons[57] and the second 1899 Hague Declaration prohibiting the use of poisonous gases in warfare.[58] (Appendix A sets out brief descriptions

[53]Owens report, 239–240.

[54]Owens report, 26. While nuclear weapons are bombs that cause damage by a sudden release of energy as some kinetic weapons do, they are not considered conventional kinetic weapons under most interpretations of international law. They are distinguished from conventional thermochemical bombs because of the wide-ranging, long-lasting (possibly for generations) effects they produce that traditional explosives do not. *Nuclear Weapons Advisory Opinion*, ¶¶35–36. This places them under the category *weapons of mass destruction*, which is also imprecise.

[55]United Nations, Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, London, Moscow and Washington, April 10, 1972, 1015 UNTS 163, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/BACF97285A9CB2A2C12563CD002D6C88/FULLTEXT/IHL-68-EN.pdf (hereafter cited as Biological Weapons Convention).

[56]Chemical Weapons Convention.

[57]Conference for the Supervision of the International Trade in Arms and Ammunition, Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, Geneva, June 17, 1925, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/921B4414B13E58B8C12563CD002D693B/FULLTEXT/IHL-36-EN.pdf (hereafter cited as Geneva Gas Protocol).

[58]Hague Peace Conferences, Declaration (IV,2) Concerning Asphyxiating Gases, The Hague, July 29, 1899, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/B0625F804A9B2A64C12563CD002D66FF/FULLTEXT/IHL-13-EN.pdf (hereafter cited as HD IV.2 (1899)).

of documents incorporating significant innovations, refinements, and extensions of international law from 1854 to 2021.) It is clear that biological and chemical attacks, though they are not kinetic in the traditional sense, are addressed by particular conventions that have become international law, and the laws of armed conflict extend to such non-kinetic attacks. Moreover, carefully crafted cyberattacks against control systems for critical infrastructure (say, a hydroelectric generating station or a natural gas pipeline) can lead to the destruction of those facilities and loss of human life.[59] If this destruction causes harm to civilians or renders critical national (civilian) infrastructure useless, the effects are indistinguishable from those of a well-placed bomb strike, and international law speaks more to the effects than the means of an attack. I will say more about these effects shortly. But if the effects of a particular means of warfare are comparable to the effects of others, and if international law already provides a way to classify kinetic and non-kinetic means of war as permissible and impermissible, then the difference Dipert sees between traditional kinetic attacks and cyberattacks is not sufficient to exempt cyber means of warfare from the international laws of armed conflict.

Indeed, the international laws of armed conflict *anticipate* novel means and methods of war. Consider the emergence of nuclear warfare. While until recently there was no similar convention to the Biological Weapons Convention or Chemical Weapons Convention that prohibits the use of nuclear weapons in war, the international community has agreed that the use of any novel weapon is subject to the international laws of armed conflict. The fourth Hague Convention of 1907 states that combatants in any international conflict among contracting parties have a duty "[t]o conduct their operations in accordance with the laws and customs of war."[60] Where such

[59] One instance known to be caused by an aggressive cyberoperation (a logic bomb) is the explosion of a pipeline in Siberia in 1982. Even though it was Soviet workers who installed the software, they unwittingly acquired the logic bomb by stealing specially crafted control software from a Canadian company. This may be more an act of sabotage and not of war, but it shows that malicious code can produce harm rising to the level of an armed attack. Owens report, 195. I thank Terry Terriff of the University of Calgary for a question about distinguishing sabotage from an armed attack and whether cyberattacks are more like sabotage. It is worth looking at in another project, but for the purposes of this one, I am following the assumption of many states that at least some cyberattacks may be considered armed attacks. I will revisit this particular incident in Chapter 5.

[60] Hague Peace Conferences, Convention (IV) Respectting the Laws and Customs of War

laws have not yet been codified, "the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience."[61] The International Court of Justice (ICJ) upheld this principle, known as the Martens Clause, in its 1996 *Nuclear Weapons Advisory Opinion*: " . . . the Court points to the Martens Clause, whose continuing existence and applicability is not to be doubted, as an affirmation that the principles and rules of humanitarian law apply to nuclear weapons."[62] Thus nuclear warfare, while it had not been addressed by specific agreements until 2017,[63] still fell under international law by the Martens Clause. Moreover, the preamble to the new Nuclear Weapons Treaty notes that "any use of nuclear weapons would be contrary to the rules of international law applicable in armed conflict, in particular the principles and rules of international humanitarian law,"[64] regardless of

---

on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, October 18, 1907, Annex, Art. 1, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/4D47F92DF3966A7EC12563CD002D6788/FULLTEXT/IHL-19-EN.pdf (hereafter cited as HC IV (1907)).

[61] HC IV (1907), preamble, qtd. in *Tallinn 2.0*, Rule 80, comment 11. A slightly different version of the Martens Clause also appears in the preamble to Hague Peace Conferences, Convention (II) with Respect to the Laws and Customs of War on Land, The Hague, July 29, 1899, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/CD0F6C83F96FB459C12563CD002D66A1/FULLTEXT/IHL-10-EN.pdf (hereafter cited as HC II (1899)), which has ben superseded, leaving the 1907 formulation as the oldest one still in effect.

[62] *Nuclear Weapons Advisory Opinion*, ¶87, quoted in Geoffrey Darnton, "Information Warfare and the Laws of War," chap. 9 in *Cyberwar, Netwar, and the Revolution in Military Affairs*, ed. Edward Halpin et al. (Basingstoke, UK: Palgrave MacMillan, 2006), 147.

[63] United Nations, Treaty on the Prohibition of Nuclear Weapons, July 7, 2017, accessed December 19, 2020, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/209/73/PDF/N1720973.pdf (hereafter cited as Nuclear Weapons Treaty). This treaty came into force for 51 states parties, none of them in possession of nuclear weapons, on January 22, 2021. The effectiveness of the terms of the treaty is still limited, since neither the nine known nuclear powers (China, the Democratic People's Republic of Korea [North Korea], France, India, Israel, Pakistan, Russia, the United Kingdom of Great Britain and Northern Ireland, and the United States of America) nor any states believed to have aspirations of becoming nuclear powers (in particular, Iran) have signalled any intention to accede to the treaty. Even so, those states are not exempt from existing international law outside the treaty.

[64] Nuclear Weapons Treaty, preamble.

the existence of the treaty. By extension, *any* novel means of warfare not otherwise addressed explicitly in international law is also subject to whatever guidance international law provides with respect to any and all means and methods of warfare. The ICJ opined, "[T]he newness of nuclear weapons has been expressly rejected as an argument against the application to them of international humanitarian law."[65] Like nuclear weapons once were, cyber weapons are also novel and not otherwise governed by specific conventions. But an analogous argument applies to cyber weapons, and it is reasonable to conclude that cyber weapons, too, are already governed by international law. Thus the novelty of cyberwarfare is not sufficient to exempt cyberwarfare from the international laws of armed conflict, either. Both of Dipert's reasons for placing cyberattacks outside the scope of international law are unsustainable.

As mentioned earlier, there is a good reason to believe that cyberattacks do properly merit consideration under the laws of armed conflict: the *scale and effects* of any damage resulting from such an attack. The ICJ introduced this notion when it ruled that the United States of America had launched an armed attack against Nicaragua in the early 1980s, even though its own armed forces were not engaged in combat.[66] It found that American sponsorship and direction of armed bands of non-Americans opposed to the Nicaraguan government[67] was equivalent to an armed attack because "its scale and effects[] would have been classified as an armed attack . . . had it

[65] *Nuclear Weapons Advisory Opinion*, ¶86.

[66] In 1979 the Sandinista National Liberation Front (named for Augusto Sandino, who led a rebellion against the American military occupation of Nicaragua during the 1920s and '30s) overthrew the dictatorial government that, had been financially supported by the USA until funding was pulled over human rights violations. Sara Chimene-Weiss et al., "Understanding the Iran-Contra Affairs: Nicaragua and Iran Timeline," Brown University, 2010, accessed May 24, 2020, `https://www.brown.edu/Research/Understanding_the_Iran_Contra_Affair/timeline-n-i.php`. The Sandinistas embraced elements of Marxist-Leninist governance, but when the new government began repressing opposition, groups of counter-revolutionaries known as *contras* formed and eventually received arms, equipment, and funding from the USA under President Ronald Reagan. It is in this context that the Sandinista government petitioned the ICJ for a finding that the American government had engaged in an illegal use of force against Nicaragua.

[67] International Court of Justice (ICJ), *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua* v. *United States of America)*, 1986 ICJ 14, June 27, 1986, ¶¶93, 100, accessed October 13, 2015, `http://www.icj-cij.org/docket/files/70/6503.pdf` (hereafter cited as *Nicaragua Judgement*).

been carried out by regular armed forces."[68] There are two main implications for cyberwarfare. First, the means and methods of aggression do not determine whether a particular action is an armed attack that justifies an armed response. A reasoned analysis of "the qualitative and quantitative factors" of the harm caused by the act of aggression—that is, a judgement about the scale and effects of the operation—is required before calling a hostile action an armed attack.[69] Since some hostile cyberoperations may cause merely a short-term inconvenience to a population, not all hostile cyberoperations can be considered armed attacks. But those that result in death and destruction quite likely are, because the harm done could reasonably also be done by other means of warfare that are readily recognized as armed attacks.[70] If the scale and effects of a cyberattack are comparable to what could result using non-cyber means, it is reasonable to conclude that the cyberattack is an armed attack for the purposes of the laws of armed conflict, and so those laws can be applied to cyberwarfare. Second, if a state contracts out the work of conducting a cyberattack to a non-state third party, that state can be deemed to be the aggressor because it sponsored and directed the work, just as the USA was held responsible for armed attacks against Nicaragua. If the scale and effects of that cyberattack are enough to justify an armed response, that response could lawfully be made against the state directing the attack.[71] Arm's-length sponsorship of a cyberattack does not mitigate responsibility for it.

The WannaCry ransomware attack that began on May 12, 2017, illustrates these points. WannaCry used a vulnerability in Microsoft Windows that had been discovered, but not disclosed to Microsoft for correction, by the USA's National Security Agency (NSA). Details of the exploit were made public on WikiLeaks in April 2017.[72] The malware was designed to take control of an unprotected computer, encrypt all of the files stored on the machine, and

[68] *Nicaragua Judgement*, ¶195, referenced in *Tallinn 2.0*, Rule 71.

[69] *Tallinn 2.0*, Rule 69, comment 1.

[70] *Tallinn 2.0*, Rule 69, comment 9.

[71] Since the attack itself may have been launched from, but not by, another state, an armed response against that other state is not readily justified under international law. A diplomatic one reminding a state of its responsibility to begin a criminal investigation of the third party's role in the cyberattack would be appropriate.

[72] Lily May Newman, "The Leaked NSA Spy Tool That Hacked the World," *Wired*, March 7, 2018, accessed December 21, 2020, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

spread to other unprotected computers.[73] Computers running Windows XP were particularly vulnerable, as updates, including malware signature updates, were no longer being provided for that version of the operating system.[74] Then it displayed a message on the screen demanding a few hundred dollars' worth of Bitcoin (a cybercurrency) in exchange for the decryption key—but not the removal of the remote access malware that was installed alongside the ransomware.[75]

WannaCry was not specifically targeted against a particular party.[76] It was indiscriminate and opportunistic. Organizations in more than 150 different countries were affected within three days of its first detection.[77] The UK's National Health Service (NHS) was particularly hard-hit: of the 236 health trusts across England, 37 were directly affected and 44 more suffered indirect effects. "[M]ore than 1,200 pieces of diagnostic equipment were infected by the ransomware, although further devices were put out of use after being disconnected from IT [information technology] systems to prevent the infection spreading."[78] While there were no patient deaths directly attributable to

[73]Norton Rose Fulbright, "WannaCry Ransomware Attack Summary," *Data Protecton Report*, May 17, 2017, accessed December 21, 2020, https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/.

[74]Newman, "The Leaked NSA Spy Tool That Hacked the World." Windows XP was first released in 2002. Microsoft's published lifecycle policy was to provide support for ten years. Microsoft Corporation, "Fixed Lifecycle Policy," April 13, 2010, accessed December 21, 2020, https://docs.microsoft.com/en-us/lifecycle/policies/fixed. Microsoft continued to issue security patches for that version of the operating system until April 2014 and malware signature updates until July 2015. Microsoft Corporation, "Support for Windows XP Ended," May 3, 2018, accessed December 21, 2020, https://www.microsoft.com/en-ca/microsoft-365/windows/end-of-windows-xp-support. Three new versions of the Windows operating system (Vista, 7, and 8) had been released by the time support for Windows XP came to an end, and Windows 10 was also available before WannaCry was unleashed. A security patch against this vulnerability was made available for these newer systems in March 2017. Microsoft later issued an emergency patch for older systems that were no longer supported.

[75]Norton Rose Fulbright, "WannaCry Ransomware Attack Summary."

[76]Gordon Corera, "NHS Cyber-Attack Was 'Launched from North Korea'," *BBC News*, June 16, 2017, accessed December 22, 2020, https://www.bbc.com/news/technology-40297493.

[77]John Kennedy, "Impact of WannaCry: MajorDisruption As Organisations Go Back to Work," *Silicon Republic*, May 15, 2017, accessed December 19, 2020, https://www.siliconrepublic.com/enterprise/wannacry-impact-organisations-attack.

[78]Owen Hughes, "WannaCry Impact on NHS Considerably Larger Than Previously Sug-

the attack,[79] more than 19 thousand appointments were cancelled—at least 130 of them for cancer screening—because of the attack.[80] Thus WannaCry had a direct, measurable impact to health care practitioners and their patients, even if the effects on patient well-being could not be measured. The estimated follow-on financial impact to the NHS for services it could provide was 5.9 million pounds (about 10.4 million Canadian dollars);[81] the cost for personnel to repair the systems would be in addition to that. Personal and financial harm extended beyond that done to the computer systems themselves.

There is a good case for thinking that North Korea was involved with the attack, though it is not sufficiently strong to assign responsibility for the harm caused by WannaCry to North Korea. Early reports from Great Britain's National Cyber Security Centre (NCSC) suggested that a group of North Korean hackers called "Lazarus" was behind the ransomware,[82] and a confident assertion of the same followed from the UK's Foreign Office after a deeper investigation.[83] Australia, Canada, Japan, New Zealand, and the USA concurred with this opinion.[84] The remaining question is whether WannaCry was developed and deployed for the North Korean government. There is insufficient evidence to confirm the suspicion that it was, in part because it acted more like a cybercriminal shakedown than an attack target-

gested," *Digital Health*, October 27, 2017, accessed December 19, 2020, https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/.

[79]Saira Ghafur et al., "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS," *NPJ Digital Medicine* 2, no. 98 (October 2, 2019): 2, accessed December 20, 2020, https://doi.org/10.1038/s41746-019-0161-6.

[80]Hughes, "WannaCry Impact on NHS Considerably Larger Than Previously Suggested."

[81]Ghafur et al., "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS," 2.

[82]Corera, "NHS Cyber-Attack Was 'Launched from North Korea'."

[83]United Kingdom Foreign & Commonwealth Office, "Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks," press release, December 19, 2017, accessed December 22, 2020, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

[84]Michael N. Schmitt and Sean Fahey, "WannaCry and the International Law of Cyberspace," *Just Security*, December 22, 2017, accessed December 19, 2020, https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/.

ing a specific state or facility.[85] However, in either case North Korea had responsibilities to the international community.

If WannaCry was not released under the control of the North Korean government, then the North Korean government had an obligation to at least attempt to put an end to the attack[86] once it became aware of the effects it was having in other states. These effects ordinarily would not be considered violations of the affected state's sovereignty because non-state actors cannot violate a state's sovereignty "unless [their] actions are attributable to a State."[87] However, WannaCry did affect the UK's sovereign right to provide health services to its citizens,[88] so it could be claimed that North Korea did not undertake the principle of due diligence to end the attack.[89]

On the other hand, if the attack was attributable to the North Korean government, things get more complicated. As social services are deemed to be an inherent function of government, the loss of functionality suffered by the NHS could be considered a violation of the UK's sovereignty under international law.[90] The harm to the UK was inflicted by cyber means, and if North Korea was in "effective control" over the Lazarus group's development and deployment of WannaCry, it could be assigned responsibility for that harm. If deaths could be attributed to the WannaCry attack, and responsibility for them to North Korea by the reasoning expressed in the *Nicaragua Judgement*, then some threshold of significant harm would have

[85] Schmitt and Fahey.

[86] *Tallinn 2.0*, Rule 2, comment 12, Rule 7, comments 2, 6, 24, 25.

[87] *Tallinn 2.0*, Rule 4, comment 2.

[88] *Tallinn 2.0*, Rule 4, comments 15, 16. Social services such as public health care are considered to be "inherently governmental functions" as a right of the state.

[89] *Tallinn 2.0*, Rule 6, comment 1, with references. One aspect of this principle is "Use your own property so as to not injure that of another." *Tallinn 2.0*, Rule 6, comment 1, note 34. While the equipment that launched or controlled WannaCry may not have been government property, any such equipment in North Korea is subject to the state's sovereignty. *Tallinn 2.0*, Rule 2, comment 1. Sovereignty over equipment imposes an obligation on the state to address the use of that equipment if it violates other states' rights. *Tallinn 2.0*, Rule 6, comments 21, 22.

[90] *Tallinn 2.0*, Rule 4, comments 13, 15, 16. Sovereignty over internal affairs and protection from forceful interference by other states are grounded in the provisions of Article 2 of the UN Charter, particularly ¶¶(1), (2), (4), and (7). There is a robust discussion over the evolving understanding of this principle, particularly with respect to universal human rights, since 1948. However, the Charter is still foundational, and the debate goes beyond the scope of this project.

been reached, perhaps even one that could be considered a "use of force" under the UN Charter. Dipert's questions revolve around issues made real by WannaCry: the means of the attack and the permissibility of a forceful response if the effects support it.

2.6 Applicability of international laws of armed conflict

I now show that Dipert's moral questions about cyberwarfare are no more challenging than their non-cyber analogues are under international law.

Dipert's third question (and one of his hard ones) about responding to a cyberattack by conventional means is probably the easiest one to address. If Dipert's question is about responding to an initial use of force using cyber means, the answer depends on the scale and effects of that use of force. If the scale and effects are comparable to what could result from an armed attack by non-cyber means, then Article 51 of the UN Charter allows a state to respond in self-defence.[91] The attack gives just cause for entering into war. However, *just cause* alone is not sufficient to justify a use of force in response. If an enemy uses a conventional means of exercising force (kinetic, but not nuclear, chemical, or biological) that reaches the level of an armed attack, then any permissible means of war may be used in response, subject to international law's *jus in bello* constraints. However, nuclear, chemical, and biological weapons can also produce the scale and effects of a kinetic armed attack (if not worse), and there is nothing in the nature of those attacks that negates a victim state's right to self-defence following those kinds of attacks.[92] If an aggressive cyberoperation against a state has the scale and effects of an armed attack then, by analogy to these other means of warfare, the state likely has just cause for responding with force.[93] Once a war has begun, the use of any conventional means of war permitted under the *jus in bello* obligations is justified. Thus Dipert's third question, "Is a *conventional* attack ever morally justified by an enemy *cyberattack*?"[94] is answered in the affirmative for both *ad bellum* and *in bello* contexts.

[91] UN Charter, Art. 51, quoted in *Tallinn 2.0*, Rule 71, comment 1.

[92] The capability to mount a counterattack is a separate question.

[93] *Tallinn 2.0*, Rule 71, comment 4, also makes this point.

[94] Dipert, "The Ethics of Cyberwarfare," 392.

Dipert's first two questions ask if a cyberattack is morally justified in response to either a conventional or cyberattack, and his fifth asks what kinds of cyberattacks are permissible once a cyber- or conventional war is in progress. It will suffice to justify the use of cyber means of war. Chemical and biological means of war are prohibited by international law because of their uncontrollable effects on humans and, to a lesser extent, the environment. They are considered "evil in themselves."[95] Unlike those kinds of weapons, the most severe effects arising from cyberweapons would not (usually) extend to the uncontrolled spread of agents harmful to human life. If this is so, then cyberweapons are not inherently evil in themselves, so international law does not prohibit their use on that ground. Further, I have already shown that the novelty of cyberweapons is not sufficient reason to prohibit them. Finally, there is nothing in international law or state practices that explicitly forbids using cyberweapons as means of warfare.[96] Consequently, if cyberattacks are permissible means of warfare—and there appears to be insufficient reason to say otherwise—then they are justified provided the *jus ad bellum* conditions and *jus in bello* obligations of the laws of armed conflict are met.

First, consider the *jus ad bellum* conditions for responding with a cyberattack. A state acting in self-defence does not need to respond—and in some cases is legally barred from responding—with the same kind of counterattack if a permissible, less destructive means of responding will end the aggression. Suppose a state launches a chemical attack against its neighbour. Using this means of war violates international law, so the victim state is prohibited under international law from responding in kind under the *no reprisals* obligation of *jus in bello*. If a kinetic counterattack will end the threat, then

[95] Orend, "War," §2.2. Orend also notes that there are other means of war that, for different reasons, are also evil in themselves. The judgement that some means of war are evil in themselves comes from the consensus declared in the Geneva Gas Protocol. It reads, in part, " . . . the use on war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices, has been justly condemned by the general opinion of the civilised world," and extends this sentiment to bacteriological weapons. These declarations are reaffirmed in the Chemical Weapons Convention and the Biological Weapons Convention. The preambles of these two conventions also affirm the desire for "the prohibition and elimination of all types of weapons of mass destruction." The preamble to the Nuclear Weapons Treaty specifically mentions "unacceptable suffering of . . . the victims of the use of nuclear weapons," which also places them in the category of "evil in themselves."

[96] *Tallinn 1.0*, 3.

using that different means of war is not only justified, but also permissible if non-forceful means cannot end the threat.[97] Moreover, the proportionality constraint may also bar responding in kind. Suppose a state makes a conventional kinetic attack against another state. If a less forceful response by diplomacy or another permissible means of war will deliver the minimum amount of force required to end the threat, then international law permits that response, but nothing more severe, such as a conventional kinetic counterstrike. For example, following the assassination of Qasam Soleimani, the head of the foreign arm of Iran's Islamic Revolutionary Guard Corps, on January 3, 2020,[98] Iran had a legitimate grievance against the USA for the harm—but perhaps not the right to an armed response, particularly since Soleimani was in Iraq at the time, so Iran itself was never threatened. Iran is not capable of winning a war against the USA at this point in time, but still perceived a need to save face by threatening a forceful retaliation.[99] A small-scale cyberattack against critical American infrastructure would be such an act, and this was one of the scenarios the US Department of Homeland Security warned about in the terrorism advisory issued the following day.[100]

Cyberweapons may provide that maximum permissible amount of force.[101] Some existing cyberweapons are very discriminating in discovering and acting on only military targets or facilities used in support of military activity.[102] These highly discriminating cyberweapons may be sufficient to put an end to a state's aggressive behaviour without being an excessive use of force. If

[97] *Tallinn 2.0*, Rule 72, comment 5.

[98] Natasha Turak, "Cyberattack and Proxy Violence Warnings As Iran Threatens 'Nightmare' Revenge against US," *CNBC*, January 7, 2020, accessed May 24, 2020, `https://www.cnbc.com/2020/01/07/how-iran-could-retaliate-against-the-us-after-solemani-killing.html`.

[99] Aniseh Tabrizi, qtd. in Turak.

[100] Department of Homeland Security [USA], *National Terrorism Advisory System Bulletin*, January 4, 2020, accessed May 24, 2020, `https://www.dhs.gov/sites/default/files/ntas/alerts/20_0104_ntas_bulletin.pdf`.

[101] The Program on Humanitarian Policy and Conflict Research at Harvard University, *HPCR Manual on International Law Applicable to Air and Missile Warfare* (New York, NY: Cambridge University Press, 2013), Rule 8 (hereafter cited as *HPCR Manual*), makes the same point concerning precision guided weapons.

[102] The best-known example is the Stuxnet virus, which sought out particular industrial controllers driving centrifuges in Iran used for enriching uranium. See Eric P. Oliver, "Stuxnet: A Case Study in Cyber Warfare," chap. 10 in Yannakogeorgos and Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 127–160.

they will provide the appropriate degree of force required to accomplish the military goal, and any other means would be excessive force, then cyberweapons ought to be preferred to those other means. This would satisfy the proportionality constraint in the *ad bellum* context better than any other means of counterattack. For this reason, a cyberattack may not only be justified in responding to either a cyber- or conventional attack. It may be the only justifiable effective response, and therefore the only one permitted by international law. Thus Dipert's questions about the permissibility of cyberattacks in response to armed attacks are also answered in the affirmative.

Second, consider the *jus in bello* obligations that apply in the context of an ongoing armed conflict. These restrictions apply to all means of war. Cyberweapons are not prohibited on the ground of being inherently evil in themselves.[103] Cyberweapons can be highly discriminating between military targets and civilian objects, and they may also satisfy the proportionality criterion with respect to achieving a military objective.[104] If no other means will accomplish the destruction or neutralisation of a military target with minimal civilian loss, then a cyberattack may be the only appropriate and permissible means to achieve a military objective. So cyberattacks may be justified in ongoing conflict situations. This answers Dipert's fifth question on what kinds of cyberattacks can be justified: those that satisfy the proportionality and discrimination constraints of *jus in bello*.

That leaves Dipert's fourth question, the other of his two hard ones: "Is a cyberattack ever morally justified in cases where the enemy has launched neither a cyber- nor a conventional attack?"[105] Like the third question, this is not as difficult as it looks. If cyberattacks are permissible in self-defence and ongoing war, they are permissible where any other kind of attack with similar anticipated effects is permissible. This reduces his question to the permissibility of a preemptive, preventive, or United Nations-approved first strike. The United Nations Charter enjoins member states to "settle their international disputes by peaceful means in such a manner that international

[103] Some *applications* of cyberweapons, such as those involving perfidy or other forms of deception intended to cause harm to persons, could be considered "evil in themselves." Such uses would be prohibited under existing international law. This is discussed in Chapter 4.

[104] Ryan Jenkins, "Is Stuxnet Physical? Does it Matter?," *Journal of Military Ethics* 12, no. 1 (April 17, 2013): 75, https://doi.org/10.1080/15027570.2013.782640.

[105] Dipert, "The Ethics of Cyberwarfare," 392.

peace and security, and justice, are not endangered" and "refrain . . . 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."[106] But the United Nations Security Council does have nominal power, at least over member states, to "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[107] Since cyberwarfare may be conducted by air, sea, or land forces broadly construed, and the United Nations Charter forms part of the international laws of armed conflict, international law answers this part of Dipert's question in the affirmative. Even so, preemptive or preventive strikes are fraught regardless of the means of attack, for they rely on presumptions concerning intent and ability. The claim that in 2003 Iraq was in possession of weapons of mass destruction was mistaken, and while there may have been just cause on other grounds to engage in armed conflict with Iraq, this was not one of them.[108] Cyberwarfare neither clarifies nor further confuses the questions around these kinds of strikes.

A preemptive or preventive cyberattack could take many forms. One attempt at a preventive cyberattack took place between 2007 and 2010 against Iran's uranium-enrichment facility at Natanz.[109] Even though this attack, called Stuxnet, infected many computers worldwide, its payload targeted a specific industrial control system with a particular configuration matching the uranium-enriching gas centrifuge cascades at Natanz.[110] These cen-

[106] UN Charter, Art. 2(2), 2(3).

[107] UN Charter, Art. 42.

[108] Glenn Kessler, "The Iraq War and WMDs: An Intelligence Failure or White House Spin?," *Washington Post*, March 22, 2019, accessed December 23, 2020, https://www.washingtonpost.com/politics/2019/03/22/iraq-war-wmds-an-intelligence-failure-or-white-house-spin/.

[109] While *preemptive* and *preventive* are similar terms, *preemptive* carries the additional sense of fending off an imminent or near-term attack. Iran was more than a few months away from launching a nuclear attack, so the strike against the Iranian facility was more a preventive measure to slow down development of nuclear weapons rather than preempting an imminent nuclear strike.

[110] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Global Politics and Strategy* 53, no. 1 (January 28, 2011): 24–5, https://doi.org/10.1080/00396338.2011.555586; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (August 2013): 383–4, 400, https://doi.org/10.1080/09636412.2013.816122. Enrichment is necessary because the most prevalent isotope of uranium, uranium-238, is not fissile; the lighter uranium-235 isotope is. Naturally-occurring uranium does not contain a

trifuges could be used to produce either lightly-enriched uranium for use in electricity-producing light-water reactors, or highly-enriched uranium for use in nuclear weapons. The lightly-enriched uranium could also be used to convert much of the uranium-238 into the fissile plutonium-239 while still producing electricity, and this plutonium could be extracted for use in nuclear weapons. Regardless of Iran's stated intentions concerning the enriched uranium, its production was taken as evidence that Iran was planning to develop nuclear weapons, and that Israel was a likely target.[111] From Israel's point of view (shared by the USA[112]), Iran's nuclear program, if it was for developing weapons, would pose an "existential threat" to the state.[113] Given that Israel had launched air strikes on nuclear facilities in Iraq in 1981 and Syria in 2007,[114] Israel would argue that a preventive strike made in self-defence was justified.[115] The Stuxnet attack was the most discriminating and proportionate means that would meet Israel's military objective, while posing less risk of harm to persons on both sides than an air strike might.[116] While this is not an argument in favour of preemptive or preventive strikes, it is evidence that cyberattacks may be the preferred method for executing such a strike. The best that can be said is this: preemptive or preventive cyberattacks are permissible if and only if preemptive or preventive strikes

---

sufficiently high proportion of uranium-235 to be used in particular kinds of reactors without increasing the ratio of uranium-235 to uranium-238. The gas centrifuges used in enrichment separate uranium hexafluoride gas containing the lighter isotope from gas containing the heavier one. An earlier version of Stuxnet manipulated the valves controlling the flow of gas between stages, varying the pressure within each centrifuge. This variant had a higher risk of causing more serious harm, including the release of radioactive material. Kim Zetter, "Stuxnet Missing Link Found, Resolves Some Mysteries Around the Cyberweapon," *Wired*, February 26, 2013, accessed December 27, 2020, `https://www.wired.com/2013/02/new-stuxnet-variant-found/`.

[111] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 28, with the observation that some Arab states also had concerns about Iran's nuclear program.

[112] Oliver, "Stuxnet: A Case Study in Cyber Warfare," 133n16.

[113] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 33; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 398.

[114] Lindsay, 398.

[115] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 33.

[116] Farwell and Rohozinski, 29; Lindsay, "Stuxnet and the Limits of Cyber Warfare," 379; Peter W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons," *Case Western Reserve Journal of International Law* 47, no. 1 (Spring 2015): 84–5, accessed December 27, 2020, `https://scholarlycommons.law.case.edu/jil/vol47/iss1/10`.

in general are permissible, and if such attacks are permissible in general, a cyberattack may be permitted where a conventional attack could not be justified. Like the rest of Dipert's questions, this question can be answered by referring to what the international community has already agreed upon.

2.7 Conclusion

I have shown that Randall Dipert's influential concerns about cyberwar and the international laws of armed conflict can be resolved or reduced to concerns about more general applications of international law. Cyberwarfare is a new development in waging war, but neither its novelty nor its differences from other means of war exclude it from the reach of current international law. If cyberwarfare is placed on the same ontological footing as other means of warfare, then international law permits, with constraints, the use of cyber means in warfare, both in self-defence and in ongoing conflict. I turn now to an examination of a particular interpretation of the international laws of armed conflict as they apply to cyberwarfare.

Chapter 3

The *Tallinn Manual*: a response to a cyberattack

3.1 Why the *Tallinn Manual*?

Evolution of international law

International law develops slowly. In contrast, warfaring technology advances rapidly, particularly when states provide funding to accelerate the process. Moreover, new interpretations of existing laws, and any necessary new laws, can only be produced in response to new developments, and not in advance of them. It is, then, no surprise that questions like Randall Dipert's, examined in Chapter 2, arise. Cyberwarfare is new and different, and opens up new possibilities for both war and peace. The international community, recognizing that cyber means and methods of war are constrained by international law, has the task of figuring out how to interpret those constraints with respect to the novel aspects of cyberwarfare. The *Tallinn Manual*[1] is a step toward filling that gap. It continues the process of codifying international law, a process that began as a result of a bloody continental war.

After the Treaty of Paris ended the Crimean War in 1856, the seven signatories (the United Kingdom of Great Britain and Ireland, the [second] French Empire, the Kingdom of Prussia, the Kingdom of Sardinia, the Austrian Empire, the Ottoman Empire, and the Russian Empire) issued the following declaration:

[1] *Tallinn 1.0*; now superseded by *Tallinn 2.0*.

The Plenipotentiaries who signed the Treaty of Paris of the thirtieth of March, one thousand eight hundred and fifty-six, assembled in Conference, —

Considering:

That maritime law, in time of war, has long been the subject of deplorable disputes;

That the uncertainty of the law and of the duties in such a matter, gives rise to differences of opinion between neutrals and belligerents which may occasion serious difficulties, and even conflicts;

That it is consequently advantageous to establish a uniform doctrine on so important a point;

That the Plenipotentiaries assembled in Congress at Paris cannot better respond to the intentions by which their Governments are animated, than by seeking to introduce into international relations fixed principles in this respect;

The above-mentioned Plenipotentiaries, being duly authorized, resolved to concert among themselves as to the means of attaining this object; and, having come to an agreement, have adopted the following solemn Declaration:

1. Privateering is, and remains, abolished;
2. The neutral flag covers enemy's goods, with the exception of contraband of war;
3. Neutral goods, with the exception of contraband of war, are not liable to capture under enemy's flag;
4. Blockades, in order to be binding, must be effective, that is to say, maintained by a force sufficient really to prevent access to the coast of the enemy.

The Governments of the undersigned Plenipotentiaries engage to bring the present Declaration to the knowledge of the States which have not taken part in the Congress of Paris, and to invite them to accede to it.

Convinced that the maxims which they now proclaim cannot but be received with gratitude by the whole world, the under-

> signed Plenipotentiaries doubt not that the efforts of their Governments to obtain the general adoption thereof, will be crowned with full success.
>
> The present Declaration is not and shall not be binding, except between those Powers who have acceded, or shall accede, to it.[2]

The Paris Declaration is arguably the first modern attempt to establish a formal international agreement on the conduct of war,[3] even though its scope is very narrow. The value of such an instrument seemed clear to the 55 states that adopted the declaration, because it established a measure of certainty concerning the treatment of their military and commercial ships should they encounter a vessel belonging to a state involved in an international war. This declaration remains in force for the still-extant states that acceded to it,[4] and its declaration concerning the effectiveness of naval blockades has become a rule of international law.[5] The significant innovations, refinements, and extensions of international law from the Paris Declaration to 2021 are set out chronologically in Appendix A as a way of capturing the evolution and acceptance of international law.

The recognized need for some consistency with respect to expected behaviour during war inspired development of these norms along two distinct but related lines: one concerning the means and methods of war (*jus in bello*), and the other concerning the humanitarian needs of the wounded—

[2]Declaration Respecting Maritime Law, Paris, April 16, 1856, accessed December 28, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/10207465E7477D90C12563CD002D65A3/FULLTEXT/IHL-1-EN.pdf (hereafter cited as Paris Declaration).

[3]It is the oldest entry in the International Committee of the Red Cross database of treaties. International Committee of the Red Cross (ICRC), "Historical Treaties and Documents: By Date," *Treaties, States Parties and Commentaries*, accessed December 28, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesHistoricalByDate.xsp.

[4]International Committee of the Red Cross (ICRC), "Declaration Respecting Maritime Law, Paris, 16 April 1856," *Treaties, States Parties and Commentaries*, accessed December 28, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=10207465E7477D90C12563CD002D65A3&action=openDocument.

[5]International Institute of Humanitarian Law, *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, ed. Louise Doswald-Beck (Cambridge, UK: Cambridge University Press, 1985), Rule 95 (hereafter cited as *San Remo Manual*).

and eventually of non-combatants in general.[6] A third line concerning both human rights and the deleterious effects of armed conflict in facilitating these rights emerged in the second half of the twentieth century.[7] The first two of these lines, along with a new consideration of *jus ad bellum*, are present in the 2013 edition of the *Tallinn Manual* (*Tallinn 1.0*); incorporating the third of these lines in the 2017 edition (*Tallinn 2.0*) is both a daring but not unreasonable innovation and an invitation to continue the implications of, and the gaps within, international human rights law as it applies in cyberspace.

The *Tallinn Manual* also continues the interpretive tradition of codifying existing international law into actionable rules of conduct for ready consultation. This practice started with the 1880 *Oxford Manual* concerning the laws of war on land,[8] and was continued by the 1994 *San Remo Manual*[9] and 2009 *HPCR Manual*[10] concerning naval and aerial warfare respectively. In the same way, *Tallinn 2.0* draws on 55 international treaties, 51 international court cases, and 58 other documents (military manuals, non-treaty resolutions and declarations, commentaries, books, and manuals analogous to the *Tallinn Manual* with respect to other domains of warfare)[11] to establish its 154 black-letter rules[12] concerning cyberoperations. With respect to form and content, the *Tallinn Manual* is both consistent with past expressions of inter-

[6] Frits Kalshoven and Liesbeth Zegveld, *Constraints on the Waging of War: An Introduction to International Humanitarian Law*, 4th ed. (Cambridge, UK: Cambridge University Press), 3, accessed December 30, 2020, https://shop.icrc.org/constraints-on-the-waging-of-war-an-introduction-to-international-humanitarian-law-pdf-en (hereafter cited as *Constraints on the Waging of War*).

[7] Universal Declaration; *Constraints on the Waging of War*, 22.

[8] Institute of International Law (IIL), The Laws of War On Land, September 9, 1880, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/40371257507EBB71C12563CD002D6676/FULLTEXT/IHL-8-EN.pdf (hereafter cited as *Oxford Manual* (1880)).

[9] International Institute of Humanitarian Law, San Remo Manual on International Law Applicable to Armed Conflicts at Sea, June 12, 1994, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/5B310CC97F166BE3C12563F6005E3E09/FULLTEXT/IHL-89-EN.pdf (hereafter cited as *San Remo Manual*).

[10] *HPCR Manual*.

[11] *Tallinn 2.0*, xxviii–xxxvii.

[12] *Black-letter rules* are "[b]asic standard rules that are generally known and free from doubt." Legal Information Institute, "Black letter law," *Wex*, accessed December 31, 2020, https://www.law.cornell.edu/wex/black_letter_law.

national law (see Appendix A) and a model for future ones.

The keepers of the Internet

I have shown that the *Tallinn Manual* is not obviously out of place in the context of international law. I turn now to showing why it is a useful and relevant contemporary expression of it.

The Internet, and cyberspace more generally, has a reputation for being a lawless domain. (Russia and China have expressed, and taken advantage of, this idea.[13]) Certainly the volume of malicious software, criminal activity, and disruptive disinformation travelling over the Internet provides some reason to think this. However, on reflection, such a claim is overbroad, even though there are calls for laws providing both more and less regulation of the Internet. On the one hand, there is little legislation or government enforcement over the content of Internet traffic. The two main exceptions come from states that have acceded to the Convention on Cybercrime,[14] or have a policy of censoring Internet traffic. On the other hand, defenders of "free speech" would like to see laws prohibiting Internet services and infrastructure companies from using vague acceptable-use policies to arbitrarily take down content that would, in a public context, have protection from government censorship.[15] The Internet may not have many explicit laws, but its operators have rules that can be applied when the threat of government regulation or the glare of public scrutiny gets uncomfortably intense. These two positions are not mutually exclusive. Protected speech does not include unlawful material such as child pornography or incitement to hatred. But addressing the concerns of parties arguing for more or less regulation is largely a matter of domestic or criminal concern, not of cyberwarfare.

[13]Thomas Wingfield (US Department of Defence and member of the international group of experts that produced *Tallinn 1.0*), qtd. in Dwight Weingarten, "International Cyber Laws Remain Work in Progress, DoD's Wingfield Says," *MeriTalk*, June 19, 2020, accessed January 18, 2021, `https://www.meritalk.com/articles/international-cyber-laws-remain-work-in-progress-dods-wingfield-says/`.

[14]Council of Europe; Patricia N. Harke, *Cyberspace: A Lawless World*, research report (Maxwell Air Force Base, AL: Air Command and Staff College, Air University, 2016), accessed January 20, 2021, `https://apps.dtic.mil/sti/pdfs/AD1041050.pdf`.

[15]Nicholas P. Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge, UK: Cambridge University Press, 2019), 8.

However, the Internet Corporation for Assigned Names and Numbers (ICANN), the not-for-profit non-governmental organization with primary responsibility for "the operational stability of the Internet" through the management of Internet addresses, the top level of the domain name system (DNS), and the "authoritative Internet DNS server system,"[16] explicitly subjects itself to international law. ICANN's Articles of Incorporation declare that it will "operate . . . in conformity with relevant principles of international law and applicable international conventions and local law."[17] This is the third ball that must pass between the two hands: there is *some* law that governs the Internet. Some of that law is international law, particularly with respect to state sovereignty over and responsibility for different physical segments of the global Internet infrastructure. Discerning *how* they apply is the problem.[18] The *Tallinn Manual* offers the first articulation of how those parts of international law apply should warfare be conducted through the Internet.

"Web War One"

The *Tallinn Manual* is a measured response to real cyberharms inflicted by international, politically-motivated, and likely state-sponsored, actors. In 2007 Estonia became the first state to face a large-scale cyberattack.[19] Estonia, having been subject to the Russification project of the Russian Empire and, after a brief period of independence, the Sovietization project of the USSR,[20] has a large Russian minority population (roughly 25% at the begin-

[16] Internet Corporation for Assigned Names and Numbers (ICANN), "Articles of Incorporation," November 21, 1998, Art. 3, accessed January 20, 2021, https://www.icann.org/resources/pages/articles-2012-02-25-en.

[17] Internet Corporation for Assigned Names and Numbers (ICANN), Art. 4; Wolfgang Kleinwächter, "International Law and Cyberspace: It's the 'How', Stupid," CircleID, December 10, 2020, accessed January 20, 2021, http://www.circleid.com/posts/20201210-international-law-and-cyberspace-its-the-how-stupid/.

[18] Kleinwächter.

[19] Helen Popp (counsellor for cyber issues, Embassy of the Republic of Estonia, Washington, DC), qtd. in Emily Tamkin, "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?," *Foreign Policy*, April 27, 2017, accessed September 7, 2019, https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

[20] Jiri Valenta and Leni Friedman Valenta, *Russia's Strategic Advantage in the Baltics: A Challenge to NATO?*, Mideast Security and Policy Studies 143, report (Ramat Gan, IL: The Begin-

ning of 2020[21]). In 1947 the USSR erected in downtown Tallinn a bronze statue of a Red Army soldier to commemorate the Soviet victory over Nazi Germany.[22] On April 27, 2007, the government of Estonia relocated the monument (with plans to also move any graves found at the memorial) to a military cemetery.[23] To the Russian ethnic minority in Estonia—and the Russian government in Moscow—this was an insult; to the Estonian majority, it was removing a painful reminder of Soviet occupation and annexation.[24]

Since reclaiming its independence in 1991 Estonia has been a pioneer in providing government services through the Internet,[25] so that by 2007 Estonian society was functionally dependent on network-based services.[26] Shortly after the statue had been moved, Estonians found that they could no longer access online government, information, or banking services.[27] This was the opening strike in what is sometimes called "Web War One."[28]

For days afterward Estonia's Internet-based services were being strangled by a *distributed denial of service* (DDOS) attack, a coordinated effort involving thousands of compromised computers around the world flooding servers inside Estonia with enough nuisance requests that they could not receive, never mind respond to, legitimate requests.[29]

Sadat Center for Strategic Studies, Bar-Ilan University, January 2018), 20, accessed January 19, 2021, https://www.jstor.org/stable/resrep16828.

[21]Statistics Estonia, "RV0222U: Population, 1 January by Year, Sex, County and Ethnic Nationality," January 1, 2020, accessed January 15, 2021, https://andmed.stat.ee/en/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV0222U/table/tableViewLayout1.

[22]Jari Tanner, "Violence Continues Over Estonia's Removal of Soviet War Statue," *Boston Globe*, April 28, 2007, accessed January 14, 2021, http://archive.boston.com/news/world/asia/articles/2007/04/28/violence_continues_over_estonias_removal_of_soviet_war_statue/; Davis, "Hackers Take Down the Most Wired Country in Europe."

[23]Tanner, "Violence Continues Over Estonia's Removal of Soviet War Statue."

[24]Davis, "Hackers Take Down the Most Wired Country in Europe."

[25]Nick Heath, "How Estonia Became an E-Government Powerhouse," *Tech Republic*, February 19, 2019, accessed January 15, 2021, https://www.techrepublic.com/article/how-estonia-became-an-e-government-powerhouse/.

[26]Tamkin, "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?"

[27]Davis, "Hackers Take Down the Most Wired Country in Europe," Tamkin, "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?"

[28]Davis, "Hackers Take Down the Most Wired Country in Europe."

[29]Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News*, April 27, 2017, accessed January 14, 2021, https://www.bbc.com/news/39655415; Tamkin, "10 Years

That was just the warm-up act. Russia commemoraties its victory in the Second World War on May 9, and the Estonians discovered that something bigger was in the works. Russian-language online chat rooms were being used to recruit and coordinate people and computers for a concentrated attack on Estonia on that day. At the stroke of midnight Moscow time, a new assault began. But Hillar Aarelaid, the head of Estonia's computer emergency response team (CERT), had recruited help from the keepers of one of the Internet's root DNS servers, the devices that direct the global routing of Internet traffic.[30] Those experts coordinated a global reactive effort to blunt 59 distinct waves of Internet traffic arriving at a rate of four million packets per second, more than enough to suffocate Estonia's network infrastructure.[31] Estonia's Internet withstood the assault, but it took the global Internet service provider network—and a great deal of trust among the high-ranking members of that community—to hold it up. And while those who took responsibility for the attack were indeed from Russia, they denied that the Russian government put them up to it, though the Russian government had no interest in putting the attack down, either.[32] Still, the weight of evidence pointed to the cyberattack on Estonia as a Russian operation, and more cyberattacks were likely to be launched against other targets.

The cyberattacks on Estonia served as a wake-up call. Cyberwar, if not already a reality, was now a very real near-term possibility. A year after the attacks, Estonia and six other European nations announced the formation of the CCDCOE, based in Tallinn, to address international and global cyber security issues and how to respond to or prevent them.[33]

Development of state policies

Around the time of the founding of the CCDCOE a number of states were developing their own strategy documents to guide their military cyberopera-

After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?"; Davis, "Hackers Take Down the Most Wired Country in Europe."

[30] Davis.

[31] Davis.

[32] Davis.

[33] NATO Cooperative Cyber Defence Centre of Excellence, "About Us," August 17, 2020, accessed January 19, 2021, `https://ccdcoe.org/about-us/`.

tions.[34] The 2010 version of the United Kingdom's national security strategy rated cyberattacks among the most significant risks to the state, a greater threat than nuclear or conventional attacks by other states.[35] Part of the USA's strategy is to assume that computing devices and networks have been breached by non-state and foreign state actors.[36] The Canadian government, while acknowledging that cyberattacks can be an effective military strategy on their own or in conjunction with other strategies,[37] recognized that cyberattacks are not equally severe, noting, "[t]he severity of a cyberattack determines the appropriate level of response and/or mitigation measures."[38] The Russian Federation considers cyberattacks within the larger framework of information warfare, which extends to "undermining the political, economic, and social system, and massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party,"[39] but it also explicitly declares that international humanitarian law applies to information war, at least with respect to limiting harm.[40]

Together these state documents capture important aspects of cyberwarfare: the threat of significant harm, the inability to trust computing systems, the inappropriateness of treating all cyberattacks in the same way, and the

[34] *Tallinn 1.0*, 2 explicitly mentions the documents produced by the USA, Canada, the UK, and the Russian Federation.

[35] Great Britain Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London, UK: The Stationary Office, October 18, 2010), 27, accessed September 9, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

[36] Department of Defense [USA], *Strategy for Operating in Cyberspace* (July 2011), 6, accessed September 9, 2019, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[37] Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa, ON: Public Safety Canada, 2010), 3, accessed September 9, 2019, http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf.

[38] Government of Canada, 2 (box).

[39] Russian Federation, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*, trans. NATO CCD COE, unofficial translation (2011), 5, accessed September 9, 2019, http://ccdcoe.eu/uploads/2018/10/Russian_Federation_unofficial_translation.pdf.

[40] Russian Federation, 6. There is also a clause that understands international humanitarian law as requiring "the establishment of special protection for information objects, which are particularly dangerous sources of technogenic catastrophes."

recognition that cyberspace is not exempt from at least some of the principles of international law. Moreover, the policy of at least some states is moving toward treating a cyberattack of "significant consequence" as an act of war, taking into account "loss of life, physical property, economic impact, and . . . foreign policy."[41]

Governments and businesses are still seeking clarity with respect to aggressive cyberoperations—both as plausible causes for military responses and as permissible operations in international dealings. The 2020 Sunburst spyware attack makes this clear. In the Sunburst attack, malicious code was injected into SolarWinds' Orion network monitoring software at build time[42] so it could be installed as part of an otherwise legitimate security update.[43] The code appears (so far) to have just exfiltrated information from Orion users, but it also gathered user login details so it could impersonate them, providing some degree of remote control over infected systems.[44] When it was discovered that several US government departments had been attacked,[45] some politicians declared that the Sunburst attack was "virtually a declaration of war"[46] that required the USA to "retaliate, and not just with sanctions."[47] Officials with actual expertise were more circumspect, but the

[41]Thomas Atkin (US Acting Assistant Secretary of Defence for Homeland Defence and Global Security), qtd. in Bryant Jordan, "US Still Has No Definition for Cyber Acts of War," *Military.com*, June 22, 2016, accessed January 18, 2021, https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html.

[42]SolarWinds Corporation, United States Security and Exchange Commission Form 8-K, December 17, 2020, accessed January 18, 2021, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/6dd04fe2-7d10-4632-89f1-eb8f932f6e94.pdf (hereafter cited as SolarWinds 8-K); Gareth Corfield, "SolarWinds Malware Was Sneaked Out of the Firm's Orion Build Environment 6 Months Before Anyone Realised It Was There—Report," *The Register*, January 12, 2021, accessed January 18, 2021, https://www.theregister.com/2021/01/12/solarwinds_tech_analysis_crowdstrike/.

[43]*Tallinn 2.0*, Rule 17, comment 7 anticipated this supply-chain attack scenario.

[44]Simon Sharwood, "SolarWinds Mess That Flared in the Holidays: Biz Confirms Malware Targeted Crocked Orion Product," *The Register*, January 4, 2021, accessed January 18, 2021, https://www.theregister.com/2021/01/04/solarwinds_malware_confirmed/.

[45]Brian Fung, "Why the US Government Hack Is Literally Keeping Security Experts Awake At Night," *CNN Business*, December 16, 2020, accessed January 18, 2021, https://www.cnn.com/2020/12/16/tech/solarwinds-orion-hack-explained/index.html.

[46]Dick Durbin (US senator), qtd. in Ian Wolfe and Brendan Pierson, "Explainer—US Government Hack: Espionage or Act of War?," *Reuters*, December 19, 2020, accessed January 18, 2021, https://www.reuters.com/article/global-cyber-legal-idUSKBN28T0HH.

[47]Marco Rubio (US senator), qtd. in Wolfe and Pierson.

suspected involvement of Russian actors has again led to a call for "a set of binding rules . . . to hold authoritarian regimes accountable, so they keep their hands off civilians in this time of peace when it comes to cyberspace."[48] A treaty would be the ideal, but as pointed out in Chapter 2, one is not likely in the near term. The *Tallinn Manual* is a step toward that desired set of rules.

Multinational support

The CCDCOE gained visibility and support quickly. The North Atlantic Treaty Organization (NATO) accredited the CCDCOE as an international military organization with subject-matter expertise "not already found within NATO"[49] only months after the centre was founded in 2008.[50] At the end of 2020 the CCDCOE included participants from 27 European nations, the USA, and the UK.[51] Even though the centre has NATO's endorsement, NATO does not fund or control the work of the centre, and the centre does not establish policy for its member states or NATO. Moreover, the CCDCOE is not a law-making body or a treaty organization. However, as an international centre of expertise, it researches and advises on cyber technology, operations, strategy, and law.[52] As such, the CCDCOE is well-equipped to do the work of analyzing and applying legal principles and practices to cyberoperations.

3.2 Constructing the *Tallinn Manuals*

Tallinn 1.0: international law and cyberwarfare

The first *Tallinn Manual* emerged from the confluence of these concurrent developments. The reality of aggressive cyberoperations and the possibility of cyberwar, the desire for clarity around states' responsibilities and rights with respect to cyberoperations, the evolution of international law in multi-

[48] Brad Smith (president of Microsoft), qtd. in Fung, "Why the US Government Hack Is Literally Keeping Security Experts Awake At Night."

[49] North Atlantic Treaty Organization (NATO), "Centres of Excellence," November 3, 2020, accessed January 19, 2021, `https://www.nato.int/cps/en/natolive/topics_68372.htm`.

[50] NATO Cooperative Cyber Defence Centre of Excellence, "About Us."

[51] NATO Cooperative Cyber Defence Centre of Excellence.

[52] NATO Cooperative Cyber Defence Centre of Excellence.

ple relevant dimensions, the tradition of codifying the current state of international law, and multinational (though not necessarily universal) interest in such a project prompted the CCDCOE to convene a meeting involving experts in international law in 2009, with the goal of identifying and setting down what parts, if any, of the existing international laws of armed conflict could reasonably be applied to cyberwarfare.[53]

Over the following three years legal, academic, and technical experts (both military and civilian) from nine states worked under the direction of Michael Schmitt to prepare a peer-reviewed manual of rules drawn from international law and an accompanying commentary explaining how those rules are relevant to cyberwarfare. Schmitt is a highly-regarded scholar of international law,[54] a participant in the drafting of the *HPCR Manual* on air and missile warfare,[55] and a pioneer in researching the relationships between cyberwarfare and international law.[56] This international group of experts agreed to the text of the rules (with any exceptions noted), and affirmed that the accompanying commentary reflected "all reasonable . . . competing views" with respect to the application of each rule.[57] In 2013 the *Tallinn Manual on the International Laws Applicable to Cyber Warfare* (*Tallinn 1.0*) was released. Unlike other domain-specific manuals on the rules of war, *Tallinn 1.0* went beyond *jus in bello* to set out some rules concerning *jus ad bellum*, analyzing what cyberoperations against a state might be just cause for a use of force in response. These are described in detail in Chapter 4 and applied to different scenarios in Chapter 5.

Tallinn 1.0 was a significant development in the attempt to pin down how existing international law applies to cyberwarfare. It addresses all of the questions raised by Dipert in his ground-breaking paper, establishing a strong argument that cyberoperations in the context of an international armed conflict are governed by the same international law governing other means and methods of warfare.

Just as important as *Tallinn 1.0* itself is for establishing how international

[53] *Tallinn 1.0*, 1.

[54] NATO Cooperative Cyber Defence Centre of Excellence, "About Us."

[55] *HPCR Manual*, 413.

[56] James E. McGhee, "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy," *Journal of Law & Cyber Warfare* 2, no. 1 (Spring 2013): 67, accessed January 25, 2021, https://www.jlcw.org/wp-content/uploads/2016/09/2013-JLCW-SpringVol_2_1.pdf.

[57] *Tallinn 1.0*, 6.

law applies are some of the criticisms it received. While none of the critics doubted the credentials each of the experts brought to the process, there were concerns that *Tallinn 1.0* represented only Western—and particularly American—interests,[58] and that *Tallinn 1.0* only codified the obvious by bolting the term *cyber-* onto already-accepted international law concerning kinetic weapons.[59]

Tallinn 2.0: Cyberoperations in peacetime

Even though these criticisms misrepresented the goals of *Tallinn 1.0*, they did not go unheeded. The sponsors of the project saw a need for interpreting other aspects of international law in the cyber context. In particular, it was observed that "States have to deal with cyber issues that lie below the use of force threshold on a daily basis,"[60] a problem that *Tallinn 1.0* did not aim to address. In 2013 the CCDCOE invited a second group of experts, again under the direction of Michael Schmitt, to assess and set down how international law controls cyberoperations more generally, particularly where state sovereignty or international obligations are implicated.

[58] Elena Chernenko, "Russia Warns Against NATO Document Legitimizing Cyberwars," *Russia Beyond*, May 29, 2013, accessed January 25, 2021, https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html; Chris Colvin, Daniel B. Garrie, and Siddartha Rao, "Cyber Warfare and the Corporate Environment," *Journal of Law & Cyber Warfare* 2, no. 1 (Spring 2013): 5–6, accessed January 25, 2021, https://www.jlcw.org/wp-content/uploads/2016/09/2013-JLCW-SpringVol_2_1.pdf; McGhee, "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy," 102; Ashley Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process," *Lawfare*, May 31, 2015, accessed January 25, 2021, https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process. While *Tallinn 1.0* aligns fairly closely with elements of American policy at the time, it diverges with respect to the severity of an initial cyberattack required to justify a use of force in response. Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal* 54 (December 2012): 15, 21–2, accessed January 25, 2021, https://harvardilj.org/wp-content/uploads/sites/15/2012/12/HILJ-Online_54_Schmitt.pdf. Chernenko's report reveals an unwillingness to believe that *Tallinn 1.0* does not reflect NATO policy. Deeks was a peer reviewer for both *Tallinn 1.0* and *Tallinn 2.0*.

[59] McGhee, "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy," 90; Lianne J. M. Boer, "'Restating the Law "As It Is"': On the Tallinn Manual and the Use of Force in Cyberspace," *Amsterdam Law Forum* 5, no. 3 (Summer 2013): 10, accessed January 25, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2338066.

[60] *Tallinn 2.0*, 1.

This renewed analysis "does not deal with international criminal law, trade law, . . . intellectual property[,] . . . private international law or domestic law,"[61] because these areas are not matters that affect a state's sovereignty over its territory. However, it does include interpretations of international law as they apply to international organizations such as NATO, the European Union, and UN agencies.[62] The revised edition clarifies the applicability of international law to peacetime cyberespionage and the non-applicability of international law to non-state actors.[63] It also includes sections on the protections afforded cyber infrastructure and operations under different international treaties concerning diplomatic practice, telecommunications, and activities at and under the sea, in the air, and in space.[64] This work required doing more than just adding *cyber-* or *electronic* to terms referring to objects or activities that do not require cyberoperations, but also setting out positions on the novel activities (for example, communicating over social media or distributing video from a civilian ship in international waters) facilitated by advances in network and computing technology.

While these are all significant expansions of the original *Tallinn Manual* in their own right, the most ambitious addition is the statement that international human rights law (at least to the extent that the treaties each state has signed, and subject to states' means to implement it) also applies to cyberoperations. *Tallinn 2.0* observes that "the principle that the same rights people have offline are to be protected online has been asserted repeatedly in numerous multilateral and multisatkeholder fora,"[65] a view that stands in concord with the one expressed by the UN Human Rights Council.[66] The sticking point is not so much that human rights law applies (even Russia and

[61] *Tallinn 2.0*, 3.

[62] *Tallinn 2.0*, Rules 32, 33.

[63] *Tallinn 2.0*, Rules 32, 33, though there are states that, under the guise of plausible deniability expressed through the "plain meaning" of words, exert control over what are officially represented as non-state actors.

[64] *Tallinn 2.0*, Rules 39–64.

[65] *Tallinn 2.0*, Rule 34, comment 1.

[66] United Nations Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, June 30, 2016, A/HRC/32/L.20, Art. 1, accessed February 11, 2021, `https://www.article19.org/data/files/Internet_Statement_Adopted.pdf` (hereafter cited as Resolution on Human Rights on the Internet).

China acknowledge the existence of the idea of human rights[67]), but how.[68] While the *Tallinn Manual* recognizes that cyber "technology is an enabler of rights,"[69] the Shanghai Cooperative Organization sees "new information and communication technologies," including cyber technology, as a threat to "international security and stability in both civil and military spheres."[70] The views expressed in the *Tallinn Manual* favour individual rights and freedoms more highly than the ones expressed in the Shanghai Cooperation Agreement, which give more power to the state to curtail individual rights, particularly with respect to access to information.[71] The positive vision of cyber technology is more in keeping with the spirit of the Resolution on Human Rights on the Internet and the open, cooperative, international nature of the Internet. I address some implications of *Tallinn 2.0*'s claim in Chapter 6.

Though the *Tallinn Manual* acknowledges the rules and commentary are the consensus opinion of the international group of experts and not the official position of any states,[72] it would be unfair to say that state representatives were not consulted during the preparation of the new edition. Drafts were presented to more than 50 "States of diverse regional backgrounds"[73] and other international organizations for unofficial comment on current states' practices with respect to international law.[74] It is important to understand that though the states and organizations that participated in this consultation were not asked to endorse the drafts or the final product, the information they provided gave better shape and nuance to the final version in such a way that it can no longer be considered purely the opinion of Western states.

Along the way, the group of experts revisited the first 9 rules, along with

[67] Shanghai Cooperation Agreement, Art. 4(1).

[68] *Tallinn 2.0*, 3.

[69] *Tallinn 2.0*, Rule 35, comment 22; *cf.* United Nations, Final Act of the International Conference on Human Rights, Teheran, April 22–May 13, 1968, A/CONF.32/41, Res. XI, preamble, p. 12, accessed February 11, 2021, `https://documents-dds-ny.un.org/doc/UNDOC/GEN/N68/958/82/PDF/N6895882.pdf?OpenElement`.

[70] Shanghai Cooperation Agreement, preamble.

[71] Shanghai Cooperation Agreement, Art. 2.

[72] *Tallinn 2.0*, 2.

[73] Burt Koenders (Minister of Foreign Affairs for the Netherlands), *Tallinn 2.0*, foreword, xxvi.

[74] *Tallinn 2.0*, 6.

26 pages of commentary, of *Tallinn 1.0* concerning state sovereignty, jurisdiction, responsibility, and countermeasures. They were replaced with 30 rules and 143 pages of commentary interpreting how international law around these concepts applies during both times of peace and times of armed conflict.[75] This expansion lays the foundation for broad individual, corporate, and state freedoms in cyberspace while respecting the (nominally) equal sovereignty customarily afforded to each state. The end result is the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,*[76] or *Tallinn 2.0*.

Toward *Tallinn 3.0*: State practice and emerging norms

The UN statute establishing the ICJ makes it clear that the court's decisions do not necessarily establish international law for parties other than the ones contesting a particular case.[77] The ICJ Statute also states that the court can draw on principles identified both in earlier cases and by "the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of law."[78] The primary source of international law is the collection of treaties between states, and those apply only to states that have agreed to be bound by them.[79] However, multinational treaties with broad acceptance are international law for more than whichever two states happen to be arguing their case before the ICJ. While the ICJ interprets these treaties with respect to particular cases and parties, the *Tallinn Manuals* interpret them with the understanding that, while they apply only to states party to them, they apply equally to each state party, so the *Tallinn Manuals* can present a codification of treaty law for general application.

The ICJ also applies international custom, determined by the degree of

[75] *Tallinn 2.0*, 2.

[76] *Tallinn 2.0*, 1–2.

[77] United Nations, Statute of the International Court of Justice, June 26, 1945, Can TS 7 (1945), Art. 59, accessed January 28, 2021, `https://www.icj-cij.org/en/statute` (hereafter cited as ICJ Statute).

[78] ICJ Statute, Art. 38(1)(d).

[79] ICJ Statute, Art. 38(1)(a).

convergence of individual states' practices,[80] in its deliberations.[81] While treaty law does not bind non-party states, states can assert by their practices that they believe some principles articulated in treaties have the weight of law (*opinio juris*).[82] Similarly, the *Tallinn Manual* treats state practice with respect to a principle as an opinion to be noted in the commentary without inferring that practices themselves necessarily establish a definitive rule capturing international law. Even so, state practices are a key to interpreting international law and identifying emerging agreement with respect to international norms.[83] Toward the end of 2020, the CCDCOE announced that work would soon begin on *Tallinn 3.0*, once again under the direction of Michael Schmitt, to do just that.[84]

Tallinn 3.0 "will reflect current State practice regarding cyber operations, including States' official statements on international law," the work of the UN's group of government experts and others on "responsible State behaviour in cyberspace," relevant academic scholarship, and "multistakeholder initiatives involving governments, industry, and civil society players."[85] It will be difficult work. Perhaps the greatest challenge to this process will be convincing states to overcome their reticence to make a substantial and candid disclosure of their practices with respect to their own cyberoperations.[86] It is far easier to object to other states' practices than admit that one's own

[80]David Kennedy, "The Sources of International Law," *American University International Law Review* 2, no. 1 (March 1987): 37n70, accessed January 25, 2021, https://digitalcommons.wcl.american.edu/auilr/vol2/iss1/1/, with references.

[81]ICJ Statute, Art. 38(1)(b).

[82]Legal Information Institute, "*Opinio juris* (international law)," *Wex*, accessed January 28, 2021, https://www.law.cornell.edu/wex/opinio_juris_(international_law). The extent to which *opinio juris* establishes international custom is unsettled, but the ICJ has the freedom to decide that a particular principle has become sufficiently customary to apply in a particular case or advisory.

[83]Weingarten, "International Cyber Laws Remain Work in Progress, DoD's Wingfield Says." Thomas Wingfield was a member of *Tallinn 1.0*'s international group of experts.

[84]NATO Cooperative Cyber Defence Centre of Excellence, "CCDCOE to Host the Tallinn Manual 3.0 Process," December 14, 2020, accessed January 18, 2021, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.

[85]NATO Cooperative Cyber Defence Centre of Excellence.

[86]Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process"; Gary Corn, "Tallinn Manual 2.0—Advancing the Conversation," *Just Security*, February 15, 2017, accessed January 25, 2021, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/; *Tallinn 2.0*, 3.

practices fall deep within what H.L.A. Hart described as the "penumbra of uncertainty."[87] If the international group of experts can succeed there, then *Tallinn 3.0* may well be considered one of "the teachings of the most highly qualified publicists of the various nations,"[88] an expression of existing international law without creating new international law. Then *Tallinn 3.0,* following in the spirit of eirenic clarification expressed by the Paris Declaration,[89] will inform further development of international law while highlighting conflicting opinions that have made negotiating a full-blown cyberspace treaty difficult.

3.3 The authority of the *Tallinn Manual*

Even though it is not a binding instrument of international law,[90] its subject matter—existing international law—is already binding.[91] This distinction appears to have been overlooked by many who referred to *Tallinn 1.0* in contexts beyond *jus ad bellum* and *jus in bello* in the cyber realm.[92] Michael Adams, a former deputy general counsel to the Chairman of the US Joint Chiefs of Staff and a 25-year veteran of the US Navy, noted that this could be because the international group of experts may have done "too good of a job":[93] the quality of the commentary is such that readers do not take note of the experts' repeated declaration[94] that the *Tallinn Manual* is not, on its own, establishing international law. Adams points out the potential consequence: "the cyber lawyer is likely to turn to the *Tallinn Manual* as the leading cyber-

[87] Michael N. Schmitt, "Cyberspace and International Law: The Penumbral Mist of Uncertainty," *Harvard Law Review Forum* 126, no. 5 (March 2013): 178, accessed January 25, 2021, https://harvardlawreview.org/wp-content/uploads/pdfs/forvol126_schmitt.pdf.

[88] ICJ Statute, Art. 38(1)(d).

[89] Paris Declaration.

[90] *Tallinn 2.0*, 2.

[91] "To the extent the Rules accurately articulate customary international law, they are binding on all States, subject to the possible existence of an exception for persistent objectors." *Tallinn 1.0*, 6; *Tallinn 2.0*, 4.

[92] Michael J. Adams, "A Warning About Tallinn 2.0 ... Whatever It Says," *Lawfare*, January 4, 2017, §1, accessed January 20, 2021, https://www.lawfareblog.com/warning-about-tallinn-20-...-whatever-it-says.

[93] Adams, §1.

[94] *Tallinn 1.0*, 1, 5, 7, 11.

warfare reference that he or she has, find the applicable rule, and restate the Manual's opinion as authoritative to the facts at hand."[95]

Tallinn 2.0's expanded scope keeps its readers from applying *jus ad bellum* and *jus in bello* principles to contexts outside of armed conflict. But it is still prone to being treated as the last, best word on international law in cyberspace when, in many regards, *Tallinn 2.0*'s commentary is the first or second comprehensive collection of the reasonable interpretations of international law. The international groups of experts hold that existing international law already supports the general statement of *Tallinn 2.0*'s black-letter rules, but the interpretations of each rule will not be consistently univocal.

To what extent, then, is the *Tallinn Manual* authoritative with respect to international law applicable to cyberoperations? The experts involved in creating the *Tallinn Manual* are highly regarded in the international legal community, either as practitioners or as scholars (and sometimes both). Their opinions, even when they disagree with each other, merit careful consideration. The text of the rules presented in the *Tallinn Manual* were, with rare noted exception, accepted unanimously by the group of experts. The international character of the group, the peer-review process, and, for *Tallinn 2.0*, the international consultation, ensure that the *Tallinn Manual* is not biased toward a particular state or alliance of states. Thus the *Tallinn Manual* carries, as a minimum, the authority of a robust, rigorous academic and legal study. With respect to settled law, the international groups of experts agreed, again as legal practitioners and scholars, that their work is not authoritative *as* law, but it is authoritative and comprehensive with respect to the ways international law may apply, either by treaty or by international custom. It is up to the states to agree on how international law applies in cyberspace, and the expert analysis of the *Tallinn Manual* enables that discussion. In the absence of such an agreement, the evolving *Tallinn Manual* may be left by default as the clearest expression of international law and the associated "penumbra of uncertainty" with respect to cyberoperations—against the desire of the groups of international experts that develop it.[96]

[95]Adams, "A Warning About Tallinn 2.0 … Whatever It Says," §2.

[96]Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process."

3.4 Conclusion

The respect and attention given to *Tallinn 1.0* is a testimony to its status as a presentation of international law. The broader international consultation that informed the creation of *Tallinn 2.0* gives assurance that it represents fairly the reasonable contrasting opinions with respect to international law in cyberspace. The announcement of *Tallinn 3.0* and some of its objectives demonstrates that the project of codifying treaty and customary international law continues to have merit, particularly as humans conduct more and more of their lives online. The *Tallinn Manual* stands as an authoritative study and representation of the current state of international law, so it is useful for understanding the rights, responsibilities, and risks that come with being a state actor in cyberspace, even as it encourages the international community to continue work on crafting acceptable norms of state behaviour in the cyber realm.

Chapter 4

The *Tallinn Manual* and just-war theory

4.1 From international law to just-war theory

The *Tallinn Manual* is regarded as a fair representation of the aspects of international law that are relevant to cyberoperations. In turn, international law, and in particular international humanitarian law, incorporate elements of just-war theory. But, as noted in Chapter 2, international humanitarian law does not incorporate *all* of just-war theory. I now turn to how well the *Tallinn Manual* accords with those criteria and requirements.

With respect to *jus in bello*, the *Tallinn Manual*'s innovation is interpreting those principles in the cyber context, following the pattern of other domain-specific manuals. *Tallinn 1.0* is the first domain-specific manual to address *jus ad bellum* conditions. *Tallinn 2.0* is the first to incorporate international human rights law, which connects to *jus post bellum*, even though *Tallinn 2.0* does not use that term. *Jus post bellum* requires that, in the process of concluding a war justly, the parties to the conflict establish the means to defend and provide for the free exercise of fundamental human rights. By incorporating human rights law, *Tallinn 2.0* sets down the plausible cyber-related aspects of a minimally just society—something which *jus post bellum*, if executed well, provides. Thus *Tallinn 2.0* incorporates at least the ultimate goal of *jus post bellum*. I now assess how closely the *Tallinn Manual* follows these aspects of just-war theory.

4.2 The *Tallinn Manual* and *jus in bello*

The largest part of the rules set down in the *Tallinn Manual* concern the conduct of an armed conflict once it has begun.[1] For the purposes of determining when an armed conflict exists, the *Tallinn Manual* follows the lead of the International Committee of the Red Cross (ICRC) set out in common Article 2 of the four Geneva Conventions: any international conflict involving the occupation of a state or hostilities between states triggers the application of international humanitarian law, regardless of whether a state of war has been declared.[2] It does not matter that the *jus ad bellum* conditions were met at the outset. Conflicts unjustly begun must still be conducted by just means.[3]

The *Tallinn Manual* interprets each the seven *jus in bello* obligations of just-war theory (see Table 2.2) in the cyber context. It makes explicit reference[4] to the Martens Clause and similar wording in other conventions asserting that the waging of war is constrained by "the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of public conscience."[5] Fol-

[1] There is no significant difference between the two editions with respect to *jus in bello*. *Tallinn 1.0* contains 76 rules associated with *jus in bello* (Rules 20–95); *Tallinn 2.0* contains 75 (rules 80–154). One new rule addressing individual responsibility under the laws of armed conflict was added, while the rules on peacekeeping operations and diplomatic protections were moved to sections containing rules that apply in times of peace as well as war.

[2] International Committee of the Red Cross (ICRC), *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd ed., ed. Knut Dörmann et al. (March 22, 2016), ¶¶193,194, 201, 202, accessed October 2, 2019, https://ihl-databases.icrc.org/ihl/full/GCI-commentary (hereafter cited as *GC I Commentary, 2016*); *Tallinn 2.0*, Rule 80, comment 2.

[3] *Tallinn 2.0*, Rule 80, comment 9, Rule 80, comments 17, 18.

[4] *Tallinn 2.0*, Rule 80, comments 11, 12.

[5] HC IV (1907), preamble; International Committee of the Red Cross (ICRC), Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, August 12, 1949, 75 UNTS 31, Art. 63, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/4825657B0C7E6BF0C12563CD002D6B0B/FULLTEXT/GC-I-EN.pdf (hereafter cited as GC I); International Committee of the Red Cross (ICRC), Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva, August 12, 1949, 75 UNTS 85, Art. 62, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2F5AA9B07AB61934C12563CD002D6B25/FULLTEXT/

lowing the guidance of the ICJ in its *Nuclear Weapons Advisory Opinion*,[6] the *Tallinn Manual* affirms "that the general rules that determine the legality of weapons will also determine the lawfulness of cyber methods and means of warfare."[7] Consequently, states have an obligation to determine how the use of cyber weapons and infrastructure stays within the bounds of *jus in bello* obligations.[8] The ICJ classifies these obligations under two "cardinal principles" with respect to means and methods: "protection of the civilian population and civilian objects," and prohibition of "unnecessary suffering of combatants."[9]

Protecting the civilian population and civilian objects

The first of these cardinal principles, the principle of *distinction* or *discrimination*, grants formal protection to civilians who are not engaged in conflicts between states. Similar protection is granted to objects and facilities that do not serve a military purpose. This protection means simply that they cannot be targets of a lawful attack, not that they cannot be harmed or damaged in the act of neutralizing a military target through a lawful attack. The *Tallinn Manual* reaffirms this principle[10] and offers guidance for determining if a potential target is a lawful objective. This protection includes a responsibility to take "constant care . . . to spare the civilian population, individual civil-

GC-II-EN.pdf (hereafter cited as GC II); International Committee of the Red Cross (ICRC), Convention (III) Relative to the Treatment of Prisoners of War, Geneva, August 12, 1949, 75 UNTS 135, Art. 142, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/77CB9983BE01D004C12563CD002D6B3E/FULLTEXT/GC-III-EN.002.pdf (hereafter cited as GC III); International Committee of the Red Cross (ICRC), Convention (IV) Relative to the Protection of Civilian Persons in Time of War. Geneva, August 12, 1949, 75 UNTS 287, Art. 158, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/AE2D398352C5B028C12563CD002D6B5C/FULLTEXT/ATTXSYRB.pdf (hereafter cited as GC IV). AP I, Art. 1(2) reads, " . . . the principles of international law derived from established custom, from the principles of humanity, and from the dictates of public conscience."

[6] *Nuclear Weapons Advisory Opinion*, ¶¶86, 87.

[7] *Tallinn 2.0*, introductory remarks to Rules 103–110.

[8] *Tallinn 2.0*, Rule 110.

[9] *Nuclear Weapons Advisory Opinion*, ¶78.

[10] *Tallinn 2.0*, Rules 93, 94, 99; *cf.* International Committee of the Red Cross (ICRC), *Rules*, Rules 1, 7.

ians, and civilian objects."[11] Persons who provide medical and chaplaincy services to those engaged in the conflict, along with the necessary equipment to support those services, are also granted protection under the terms of the Geneva Conventions and Additional Protocols.[12] Importantly, this protection extends to "[c]omputers, computer networks, and data that form an important part of the operations or administration of medical units and transports," provided that the same equipment is not used to support military activity against the opposing parties.[13] This is an important clarification, because it extends to personal data relevant to patient care.[14] Protecting patient data benefits all parties in the conflict because it helps medical staff provide the benevolent treatment owed to any prisoners of war.[15] This is the first time data is explicitly given protection separate from its underlying storage and processing technology. I will take up the implications of this in Chapter 6.

Another application of the principle of distinction involves infrastructure that facilitates intercontinental cyberoperations. This draws in multiple criteria for distinguishing the lawfulness of targeting long-range infrastructure during an armed conflict: what is it being used for, who owns it, and what non-belligerent states are making legitimate use of it? One kind of long-range cyber infrastructure is the undersea cable.[16] The *Tallinn Manual* notes that, under the principle of distinction with respect to non-belligerents, undersea cables are protected objects. Many undersea communication cables are owned by private groups, even though they are used (in part) for government purposes;[17] thus they are technically civilian objects. Further, they terminate in two different states (and may cross the continental shelf that belongs to other states),[18] so the cables are governed by multiple govern-

[11] *Tallinn 2.0*, Rule 114.

[12] *Tallinn 2.0*, Rule 131.

[13] *Tallinn 2.0*, Rule 132.

[14] *Tallinn 2.0*, Rule 132, comment 3.

[15] *Tallinn 2.0*, Rule 135, comments 2–4; *cf.* International Committee of the Red Cross (ICRC), *Rules*, Art. 109–11.

[16] Data can also be transmitted using satellite links. The laws of war around satellite communications are less clear, because they involve both space and international telecommunications law. *Tallinn 2.0*, 272–73. Some of the open questions will be presented in Chapter 7.

[17] *Tallinn 2.0*, Rule 54, comment 2.

[18] *Tallinn 2.0*, Rule 54, comments 6, 10; *cf.* United Nations, Convention on the Law of the

ments' territorial authority as well as the Convention on the Law of the Sea (CLOS).[19] For the most part, then, cables cannot be lawfully disrupted, for

> it would be incongruent to provide States a right to lay such cables without a corresponding obligation on the part of other States to protect them. Thus, for instance, the Law of The Sea does not provide a legal basis for a State to cut another State's submarine fibre optic cable in order to reduce trans-continental Internet traffic in times of tension.[20]

There are two possible lawful exceptions, only one of which is detailed in the *Tallinn Manual*. If a state has become an "Occupying Power" over territory containing a submarine communication cable, and that cable is connected to neutral territory, then it may "be seized or destroyed [only] in the case of absolute necessity."[21] The other exception is found in the *San Remo Manual*: submarine communication cables in areas "beyond national jurisdiction" and that "do not exclusively serve the belligerents" must be given particular care against damage.[22] If it can be ascertained that only belligerent states are using the cable (both a high technical bar and an improbable scenario with respect to Internet traffic) for military purposes, it might then be a legitimate military objective subject to lawful attack.[23]

The Russia-based shutdown of Estonia's Internet, even if it had been a military response to an actual use of force on Estonia's part (and the moving of a statue is not one), clearly flouts the principle of discrimination. The cyberattack affected the whole country, not just the Estonian military forces. Civilians had no access to banking or government services, for even if they had gone to a branch or an office for in-person service, the person behind the counter could well not have been able to satisfy the request because their workstation used the public Internet. Civilian persons and infrastructure

Sea, December 10, 1982, 1833 UNTS 3, Art. 79, 87(1)(c), 87(2), 112(1), accessed November 28, 2019, `https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf` (hereafter cited as CLOS).

[19] *Tallinn 2.0*, Rule 54, comment 1.

[20] *Tallinn 2.0*, Rule 54, comment 15.

[21] *Tallinn 2.0*, Rule 149, comment 10; *cf.* HC IV (1907), Annex, Art. 54. Compensation is required as part of establishing peace.

[22] *San Remo Manual*, Art. 36, 37.

[23] *Tallinn 2.0*, Rule 150, comment 5.

were the cyberattack's intended targets. The harm they suffered was direct, not incidental to an attack on a military target.

Prohibition of unnecessary suffering

The cardinal principle of avoiding unnecessary suffering is also relevant to cyberwarfare. One way to avoid unnecessary suffering is to abide by the principle of distinction, thereby limiting the effects of an aggressive cyberoperation to lawful targets. However, even the lawful harm done to combatants is limited to what is justifiably necessary (that is, proportionate) to render them unable to continue in the conflict.[24] The *Tallinn Manual* notes that, for the most part, cyberattacks will not inflict this kind of unnecessary suffering.[25] Even so, there are some cyberattacks that can fall under the category of means and methods *mala in se* (that is, *evil in themselves*). The data connection built in to personal assistive devices (for example, pacemakers, insulin pumps, prosthetic limbs, or cochlear implants) provides an avenue for a cyberattack to take control of that device and use it to inflict more harm than required to render the person unable to participate any further in the conflict.[26] In addition, cyberattacks that are designed to be indiscriminate with respect to civilian targets (persons or objects) are prohibited,[27] as are "cyber booby traps," pieces of software designed to result in death or injury that is unexpected by the person triggering it. To count as a booby trap, this software has to be associated with a limited class of objects that appear innocuous to a "reasonable observer": medical equipment, items used for training or caring for children (including toys), kitchen utensils or appliances, or objects associated with cultural or spiritual heritage.[28] As an example, consider malware deployed to an Internet-connected game console. After a triggering condition is met (perhaps time, a sequence of button presses, or a number of interactions), the malware modifies the signals that activate the feedback mechanism in the controller. These signals induce rapid overheating in the controller so it catches fire, burning the player. This

[24] *Nuclear Weapons Advisory Opinion*, ¶78.
[25] *Tallinn 2.0*, Rule 104, comment 6.
[26] *Tallinn 2.0*, Rule 104, comment 6.
[27] *Tallinn 2.0*, Rule 105.
[28] *Tallinn 2.0*, Rule 106, comment 3.

would be a cyber booby-trap, and thus a violation of both the principle of distinction and the principle of avoiding unnecessary suffering.

Further, the *Tallinn Manual* points out that cyberattacks designed "for the exclusive purpose of disrupting transportation of food to civilian population centres" or "target[ing] food processing and storage facilities in order to cause civilian food stocks to spoil"[29] are prohibited because they are intended to starve civilians, not weaken the enemy's military personnel.[30] In a similar vein, the natural environment[31] has protected status both under the principle of distinction as a civilian object and under the principle of proportionality should some part of it be used in support of a state's military activity.[32] The *Tallinn Manual* only affirms that the natural environment is a civilian object,[33] noting that signatories to AP I have additional obligations to not use "cyber methods or means of warfare which are intended, or may be expected, to cause widespread, long-term, and severe damage to the natural environment."[34] This points to a developing recognition that using environmental harm as a means of war against a civilian population can have the same effect as using starvation or otherwise depriving the civilian population of the means of subsistence, and so could justifiably be included in the category of methods *mala in se*. A cyberattack that results in this kind of harm, such as causing a rupture in an oil pipeline where it crosses an aquifer, would qualify as such a prohibited attack.

Children receive specific consideration with respect to armed conflict in the *Tallinn Manual*. The use of child soldiers is considered a war crime and

[29] *Tallinn 2.0*, Rule 107, comment 4.

[30] International Committee of the Red Cross (ICRC), *Rules*, Rule 53.

[31] The term *natural environment* does not have an agreed-upon definition within international law. *Tallinn 2.0*, Rule 143, comment 3 follows United Nations, Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, December 10, 1976, 1108 UNTS 151, Art. II, accessed November 26, 2019, `https://treaties.un.org/doc/Treaties/1978/10/19781005%2000-39%20AM/Ch_XXVI_01p.pdf` (hereafter cited as ENMOD): "the dynamics, composition or structure of the Earth, including its biota, lithosphere, hydrosphere and atmosphere." ENMOD includes outer space, but the *Tallinn Manual* committee did not have consensus on this point.

[32] *Tallinn 2.0*, Rule 143, comment 4; *cf.* GC IV, Art. 147 ("extensive destruction and appropriation of property not justified by military necessity and carried out unlawfully and wantonly"); International Committee of the Red Cross (ICRC), *Rules*, Rules 43–45.

[33] *Tallinn 2.0*, Rule 143(a).

[34] *Tallinn 2.0*, Rule 143(b).

an offence against the rights of children, and is therefore prohibited under accepted international law.[35] The *Tallinn Manual* extends this prohibition to the cyber domain: "[s]tates must . . . take all feasible measures to ensure that children do not participate in hostilities. . . . There is no reason to exclude engaging in cyber activities from the ambit of participation."[36]

This is a reasonable position to advance. For example, convincing a child to follow a set of instructions that launch a DDOS attack against a network (without the child knowing that the network belongs to a hospital system) because it would be a fun learning experience seems less serious than sending a child soldier into armed combat. However, it is just as exploitive and just as great a violation of the child's rights for a child to be used as a cyber warrior as it is for that child to be sent to shoot up a school or movie theatre. Any involvement of children in combat is prohibited as exploitive.[37] In a way, it is also perfidious:[38] it takes advantage of other states acting in good faith to mitigate harm to children, leveraging that protection to achieve a military objective against a state acting in good faith. Further, this places the children at greater risk of harm. Any children participating in hostilities by cyber means become combatants, and so become legitimate targets for attack.

The proportionality obligation of *jus in bello*, understood as the avoidance of excessive force or harm,[39] can also be slotted under this rubric of avoiding unnecessary suffering, because those requirements align with two distinct aspects arising from the principle of distinction. The first is intended to protect lawful combatants. Any suffering inflicted upon enemy combatants is limited to that caused by the minimum justifiable force (using permissible means and methods) required to render the targeted part of the enemy's military capability ineffective.[40] The second aspect establishes the same restriction with respect to civilian harm, at least for adherents to AP I.[41] The

[35] International Committee of the Red Cross (ICRC), *Rules*, Rules 136, 137; *cf.* Rights of the Child, Art. 38.

[36] *Tallinn 2.0*, Rule 138, comment 4.

[37] Rights of the Child, Art. 36.

[38] International Committee of the Red Cross (ICRC), *Rules*, Rule 65.

[39] *Tallinn 2.0*, Rule 113, comment 1.

[40] International Committee of the Red Cross (ICRC), *Rules*, Rule 70, comment on pp. 240–241.

[41] International Committee of the Red Cross (ICRC), *Rules*, Rule 14; *cf.* AP I, Art. 51(5)(b),

Tallinn Manual acknowledges this constraint for cyber means and methods with respect to both combatants and civilians.[42]

Finally, in the spirit of not responding to an injustice with another injustice, the limits on reprisals against states that do violate the other *jus in bello* obligations are intended to serve as additional safeguards against unnecessary suffering. The Geneva Conventions affirm that "[t]he High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances."[43] This expectation extends to the whole of international humanitarian law as it has developed since then,[44] regardless of how closely other parties to the conflict adhere to them.[45] While the prohibition of reprisals against civilians is not yet taken as international law, it does apply to the states that have signed or acceded to AP I.[46] There is also a growing recognition that reprisals, even when targeted against belligerents only and not civilians, are ineffective in curtailing delinquent behaviour,[47] and that reprisals made against civilians often lead to escalating counter-reprisals.[48]

The *Tallinn Manual* follows the current state of international law and not the full *jus in bello* obligations of just-war theory in this regard. It acknowledges that reprisals made by cyber means against civilian targets may not be carried out by the states party to AP I that have not issued a reservation or alternative understanding against this prohibition.[49] Any cyber-based reprisals against belligerents are limited to government-approved actions of last resort "for the purpose of inducing the adversary to comply with the law."[50] In other words, reprisals are not meant to be punitive but coercive, though the state on the receiving end of them will likely treat them

---

57(2)(a)(iii), 57(2)(b). There is increasing recognition that this rule has become part of international law applicable to all states, not just the states party to AP I. International Committee of the Red Cross (ICRC), *Rules*, Rule 14, commentary on pp. 47–48.

[42] *Tallinn 2.0*, Rule 104, comments 2, 3, Rule 113.

[43] GC I–IV (1949), Common Art. 1.

[44] International Committee of the Red Cross (ICRC), *Rules*, Rule 139.

[45] International Committee of the Red Cross (ICRC), Rule 140.

[46] International Committee of the Red Cross (ICRC), *Rules*, Rule 146, commentary on p. 520; AP I, Art. 51(6).

[47] International Committee of the Red Cross (ICRC), *Rules*, Rule 145, commentary on p. 514.

[48] International Committee of the Red Cross (ICRC), Rule 146, commentary on p. 522.

[49] *Tallinn 2.0*, Rule 109, comment 1.

[50] *Tallinn 2.0*, Rule 108, comment 5.

as punitive. Even so, the *jus in bello* obligation to avoid unnecessary suffering, the commitment of many states to refrain from reprisals for violation of international law, and the observed escalation of ineffective reprisals argue in favour of this prohibition eventually becoming accepted as international law.[51]

There is a real-world example of a cyberattack causing unnecessary suffering. WannaCry (described in Chapter 2), if it had been definitively attributable to the North Korean government, would fall afoul of the principle of avoiding unnecessary suffering as well as the principle of discrimination. While no deaths were attributable to WannaCry in the UK, the malware did affect civilians waiting for treatment, and for patients whose conditions produced suffering, it prolonged that suffering unnecessarily. In the context of an armed conflict, this could have been prosecuted as a war crime, one committed by cyber means, for it would have been a grave breach of international humanitarian law.[52]

Respect for rights of citizens

All of the foregoing *jus in bello* obligations are focused on the protections that apply to combatants and civilians from an enemy or neutral state. The remaining one, articulated in part in GC IV, focuses on a belligerent state's treatment of non-combatants under its protection: a state at war must respect at least some rights of *all* non-combatants, including its own citizens, within its own territory or any other territory it occupies:

> Protected persons are entitled, in all circumstances, to respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs. They shall at all times be humanely treated, and shall be protected especially against all acts of violence or threats thereof and against insults and public curiosity.
>
> . . . [A]ll protected persons shall be treated with the same consideration by the Party to the conflict in whose power they are,

[51] International Committee of the Red Cross (ICRC), *Rules*, Rule 145, commentary on p. 513.

[52] International Committee of the Red Cross (ICRC), Rule 90.

> without any adverse distinction based, in particular, on race, religion or political opinion.
>
> However, the Parties to the conflict may take such measures of control and security in regards to protected persons as may be necessary as a result of the war.[53]

This is a minimal set of rights. Despite the existence of the Universal Declaration of Human Rights, the human rights treaties that refer to it (such as the International Covenant on Civil and Political Rights [ICCPR], the International Covenant on Economic, Social and Political Rights [ICESCR],[54] and other regional treaties) protect different, but overlapping, sets of rights. These treaties also impose differing obligations with respect to facilitating the exercise of those rights, and may permit suspending a very few rights on a temporary basis in times of declared national emergency.[55] This process is called *derogation*, though the matter of which rights may be suspended and what reasons justify that suspension is very much not settled. Treaty law makes it clear that any derogation from rights is discouraged, as most rights treaties contain language upholding all non-derogation clauses in other rights treaties to which a state is party.[56] In other words, if a right is non-derogable under one rights treaty, it is also non-derogable under all applicable rights treaties.

Despite the lack of agreement in treaty law concerning which rights are inviolable and which ones states may derogate from,[57] the *Tallinn Manual* asserts that whatever human rights a person enjoys in meatspace[58] also extend to cyberspace.[59] The *Tallinn Manual* articulates not just respect for human rights in a cyber context,[60] but also a state's obligation to protect them in

[53] GC IV, Art. 27.

[54] United Nations General Assembly, International Covenant on Economic, Social and Cultural Rights, December 16, 1966, 993 UNTS 3, accessed June 26, 2018, `https://treaties.un.org/doc/Treaties/1976/01/19760103%2009-57%20PM/Ch_IV_03.pdf` (hereafter cited as ICESCR).

[55] *Tallinn 2.0*, introductory comments to Rules 34–38, pp. 179–82; ICCPR, Art. 4.

[56] ICCPR, Art. 5; ICESCR, Art. 5.

[57] *Tallinn 2.0*, Rule 38.

[58] *Meatspace* is a colloquial term used by some people in the computing industry to refer to things and activities outside of cyberspace.

[59] *Tallinn 2.0*, Rules 34, 35.

[60] *Tallinn 2.0*, Rule 34, comment 1.

cyberspace.[61] This protection is understood as the obligation to "ensure respect for" rights by not engaging in unlawful interference against them.[62] Some rights are particularly important in the cyber context: "freedom of expression, privacy, freedom of opinion, and due process."[63] These are appropriate extensions of rights associated with older public and private forms of communication. However, some treaties permit all but due process and freedom of opinion to be curtailed "to the extent required by the exigencies of the situation" should a significant threat to the "life of the nation" arise,[64] and this is also acknowledged in the *Tallinn Manual*.[65] The upshot is that, even in times of armed conflict, the *Tallinn Manual* asserts, with reasons and qualifications, that there are *some* human rights that states are obliged to protect in cyberspace as well as in meatspace during times of armed conflict. The matter of human rights comes up again with respect to *jus post bellum*.

4.3 The *Tallinn Manual* and *jus ad bellum*

Determining when an armed conflict may be justly begun is maddeningly difficult. Under the UN Charter, this is a matter for the United Nations Security Council to decide,[66] a time-consuming process often frustrated by the competing interests of its permanent members. There is one exception permitted: a state may declare unilaterally that it is acting in self-defence against a use of force by another state.[67] The UN Charter does not consider a plausible threat of a use of force to be sufficient ground for a state to launch a pre-emptive strike in self-defence without the consent of the Security Council.[68]

[61] *Tallinn 2.0*, Rule 36, comment 1.

[62] *Tallinn 2.0*, comment 5, introduction to Rules 34–38, p. 181.

[63] *Tallinn 2.0*, Rule 35, comment 1.

[64] ICCPR, Art. 4(1).

[65] *Tallinn 2.0*, Rule 38.

[66] UN Charter, Art. 39.

[67] UN Charter, Art. 51.

[68] UN Charter, Art. 39–42. Brian Orend puts this idea bluntly: "The mere *threat* of war, and the presence of mutual disdain between two communities, do not suffice as indicators of war." Orend, "War." Some states do not accept this restriction, and there may be some situations where the protection of civilians might provide just cause for an armed attack against a state that does not honour the rights of its civilians under the emerging doctrine of *responsibility to protect*. Gareth Evans et al., *The Responsibilty to Protect: Report of the Interna-*

The *Tallinn Manual* aims to provide guidance on how an aggressive cyberoperation can justly be declared a *use of force* or an *armed attack*. The UN Charter is not helpful here, since it neither defines nor clearly describes what a *use of force* or an *armed attack* is.[69] This draws in the idea of *just cause*, one of the *jus ad bellum* conditions (see Table 2.1) that must be satisfied to justify engaging in an armed conflict. The *Tallinn Manual* proposes eight criteria, set out in Table 4.1, to consider when making this determination.[70] This study is particularly interested in four of these: *severity*, *immediacy*, *directness*, and *measurability of effects*. Should there be enough evidence to declare the initial aggressive act a use of force or an armed attack, the target state has just cause for responding, but only in accordance with the other *jus ad bellum* conditions. For example, even if a state has demonstrated that there is just cause for a forceful response, the methods that do not satisfy the proportionality constraint are not lawful responses.

It may not be possible to precisely determine the severity of any harmful effects caused by a use of force. However, some of the effects can be compared to those produced by other uses of force that have already been judged to be armed attacks. This is part of assessing what the ICJ has labelled the *scale and effects* of the action.[71] The *Tallinn Manual*'s *severity* and *measurability of effects* criteria for establishing just cause are intended to capture this important idea.[72] *Immediacy* and *directness* look at the causes of those effects. The first concerns the amount of time between the primary cause leading to

---

tional Commission on Intervention and State Sovereignty (Ottawa, ON: International Development Research Centre, 2001) (hereafter cited as Responsibility to Protect).

[69] *Tallinn 2.0*, Rule 69, comment 2. The UN Charter only preserves the right of a state to respond in self-defence to an armed attack. UN Charter, Art. 51. Otherwise, unless the UN Security Council has decided that the use of force is justified, the Charter enjoins member states to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state . . . " UN Charter, Art. 2(4).

[70] *Tallinn 2.0*, Rule 69, comment 9. The *Tallinn Manual* provides a minimal list that includes the six criteria proposed in Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37, no. 3 (1999): 914–15, `https://heinonline.org/HOL/Page?handle=hein.journals/cjtl37&id=893`. It further notes that other factors may be taken into account depending on the political context. *Tallinn 2.0*, Rule 69, comment 10. This leaves it open for the target state, and not the international community, to determine whether an armed response is justified.

[71] *Nicaragua Judgement*, ¶195; *Tallinn 2.0*, Rule 71, comment 7.

[72] *Tallinn 2.0*, Rule 71, comment 8 makes indirect reference to these criteria.

	Cyber just-cause criteria[a]
severity	"scope, duration, and intensity" of harm to state interests; physical damage to objects and injury or death of humans are most severe
immediacy[b]	rapid progress of consequences
directness[b]	clear, proximate causal connection of attack to its effects
invasiveness[b]	degree of effect on target state's interests and degree of effort required to produce them
measurability of effects	objectively quantifiable description of extent of damage
military character[b]	carried out by a state military organization, targets a military system, or increases the effectiveness of an armed attack
state involvement	participation or support from an organ of the state in the development and execution of the attack
presumptive legality	qualitative assessment of similarity to operations that have clearly been determined are not uses of force or are not barred by international law

Table 4.1: Cyber just-cause criteria. All of these criteria must be evaluated before making a forceful response to a cyberattack. No single one is decisive with respect to classifying the action as a use of force; conversely, failure to meet certain criteria does not necessarily rule out such a classification.

[a] Summarized from Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge, UK: Cambridge University Press, 2017), Rule 69, comment 9 (hereafter cited as *Tallinn 2.0*).

[b] Failure on this criterion is not necessarily decisive.

the effects, and the second concerns the length and complexity of the causal chain itself. I explore the relationships among these four criteria further in Chapter 5.

The four remaining qualitative just-cause criteria are *military character*, *state involvement*, *invasiveness*, and *presumptive legality*.[73] Each of these is a little more nuanced in the cyber context than in the context of conventional warfare.

Military character

An aggressive cyberoperation is more likely to be considered to have military character when a state's armed forces have some degree of involvement in launching or facilitating the cyberoperation, or when the target serves a military purpose.[74] In conventional warfare the involvement of a state's armed forces is usually readily visible because the combatants, vehicles, vessels, and aircraft are expected to display, at least in most circumstances, some mark identifying them as belonging to a military force.[75] In contrast, determining whether a state's armed forces are involved in a cyberattack may be difficult to do quickly. (Edward Cardon of US Cyber Command has noted that military character and state involvement may be easier to determine than is commonly believed. He recalled that, while US Cyber Command was preparing a cyberattack to curtail *Daesh*'s Internet presence in 2016, intelligence experts preferring subtle disruption "would say, 'If you do it like that, they'll know it's you!' . . . I'd just look at them and say, 'Who cares? When I'm using artillery, attack aviation, jets—you think they don't know it's the United States of America?"[76]) However if, on the basis of available evidence, the cyberattack appears to have a military origin, then it is more likely to be a just cause for an armed response than if there is no such involvement, just as it is in conventional armed conflict.

A cyberattack definitively targeting a military facility, such as Israel's hacking of Syria's air defences as part of a strike against a potential nuclear

[73] *Tallinn 2.0*, Rule 69, comment 9.

[74] *Tallinn 2.0*, Rule 69, comment 9(f).

[75] HC IV (1907), Annex, Art. 1; *San Remo Manual*, Art. 110; *HPCR Manual*, Art. 1(x); AP I, Art. 44(3).

[76] Garrett N. Graff, "The Man Who Speaks Softly—and Commands a Big Cyber Army," *Wired*, October 13, 2020, §5, accessed October 14, 2020, `https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/`.

facility in 2007,[77] also satisfies the military character criterion for having just cause. If a military facility is the target of a cyberattack by activist or criminal groups, the military character criterion is again satisfied, but without state involvement (at least at the outset) the attack is not likely a use of force under the terms of international law.[78] On the other hand, the 2007 cyberattack on Estonia did not explicitly target a military facility, and it was not clearly connected to Russian armed forces, so that attack did not have a clear military character. Yet the attack was still severe enough to merit consideration as a use of force against Estonia. All this demonstrates that failing to meet the military character criterion is not, by itself, sufficient reason to judge a cyberattack as not being a just cause for a use of force in response.

State involvement

If an aggressive cyberoperation is directly connected to a military organization, it is sufficient to satisfy the criterion of state involvement in the attack. However, it is not a necessary condition for finding a foreign state's involvement, in part because states can contract out the disruptive dirty work. This is easier to do in the cyber realm than in the realm of land-based combat, but it is a land-based conflict that established this principle: the American support for the *contras* against the Sandinista government of Nicaragua in the 1980s.[79] While the armed forces of the USA were not active participants in the ground-based aspect of the conflict, the USA funded, trained, and equipped the rebel forces that did participate. The ICJ ruling observed that

> while the arming and training of the *contras* can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily so with respect to all of the assistance given by the United States Government. In particular, . . . the mere supply of funds to the *contras*, while undoubtedly an act of interven-

[77] Sharon Weinberger, "How Israel Spoofed Syria's Air Defence System," *Wired*, October 4, 2007, accessed February 1, 2021, `https://www.wired.com/2007/10/how-israel-spoo/`.

[78] This does not mean that the state from which the attack was launched has no responsibility to end it. *Tallinn 2.0*, Rule 6.

[79] Chimene-Weiss et al., "Understanding the Iran-Contra Affairs: Nicaragua and Iran Timeline"; see also the summary in Chapter 2 on p. 31.

> tion into the internal affairs of Nicaragua, . . . does not in itself amount to a use of force.[80]

By analogy, even though a state organization may not be involved directly or immediately in an aggressive cyberoperation (say, one mounted by a skilled activist group), if it can be shown that there is a connection to a state body, such as providing training or equipment to the aggressors that enabled them to carry out an attack (something more than funding), then the criterion of state involvement in the particular operation might also be met.[81] This kind of connection would weigh in favour of judging the action as meeting the threshold of a use of force, and thus more likely to provide just cause for a forceful response. In a similar vein, if a state provides sanctuary to such a group while leaving it to its own devices to launch a cyberattack against another state, the sheltering state has not made a use of force, but failing to take steps to end the attack is likely a violation of the target state's sovereignty[82] through a failure of due diligence.[83] In other words, while money and shelter may be instrumental to launching an aggressive cyberattack, they are not the means of carrying out any attack. Merely providing these things to a group is not sufficient to demonstrate state involvement in the attack itself. Considering an armed response on this basis alone amounts to acting on hearsay, not direct evidence connected to the cyberoperation. On the other hand, equipping and training are strong indicators of some kind of state sponsorship. For example, while the Russian nationalist activists who acknowledged their part in the 2007 cyberattack on Estonia denied receiving state funding, training or direction,[84] the Sandworm group of Russian hackers responsible for the NotPetya malware that did an estimated US$10 billion worth of damage worldwide in 2017,[85] was not

[80] *Nicaragua Judgement*, ¶228.

[81] *Tallinn 2.0*, Rule 69, comment 4.

[82] *Tallinn 2.0*, Rules 6, 7.

[83] *Tallinn 2.0*, Rule 69, comment 5.

[84] Davis, "Hackers Take Down the Most Wired Country in Europe."

[85] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, accessed February 4, 2021, `https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/`. Like the Sunburst attack, NotPetya was injected into a Ukranian software developer's build system and was released through a legitimate piece of accounting software. It spread rapidly, encrypting hard drives on every system it could get into, but unlike other encryption attacks,

known to have a verified association with the Russian government, so state involvement could not be asserted. However, the discovery that Sandworm was part of Russia's GRU (Chief Intelligence Office)[86] changed that: NotPetya is now widely recognized as a state-sponsored cyberattack, and six members of Sandworm have been indicted in the USA for their involvement in NotPetya.[87]

Invasiveness

Even in cases where there is evidence of state involvement in an aggressive cyberoperation, that operation has to intrude on a state's sovereignty in some significant way in order to be considered a use of force under the *Tallinn Manual*'s interpretation of just cause. Invasiveness is difficult to assess, because if a cyberoperation's only effect is exfiltration of data, then the action is only at the level of espionage, which is permissible under international law,[88] even though it required invading a system in the target state to get that information. If there is no effect more severe than exfiltration of data or unauthorized access to a system within the targeted state, the operation is not considered invasive, and the right to an armed response is not triggered. However, the invasiveness criterion is not a simple *yes* or *no* test based on the absence or presence of harm done to the system. If there is a more severe effect on the system, then invasiveness is to be understood as a matter of degree, not in absolute terms.[89] A cyberoperation directed against a family's media server (for example) would not be considered invasive with respect to state interests, but one directed against a power generation plant or a military facility might be considered highly invasive, depending on the efforts that had been made to secure the computing systems before the attack was

---

it did not provide a way to decrypt the drives.

[86] Ellen Nakashima, "Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 12, 2018, accessed February 4, 2021, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[87] Andy Greenberg, "US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit," *Wired*, October 19, 2020, accessed February 4, 2021, https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/.

[88] *Tallinn 2.0*, Rule 69, comment 9(d).

[89] *Tallinn 2.0*, Rule 69, comment 9(d).

launched.[90] In contrast, if a system has been left vulnerable to exploitation, as the UK's NHS had been when they were struck by WannaCry (see Chapter 2), little effort or planning is needed to disable that system. It is hard to claim invasiveness when the door to a targeted system is left wide open for anyone with the inclination to disrupt the system to do so readily.[91]

The more secure a system is, the greater effort required to disrupt its operation. Just as it takes a great deal of planning and circumvention of security systems to steal a 100-kilogram gold coin from a museum (even with low-technology methods),[92] disruptions of systems with strong cybersecurity indicate a degree of intent and planning on the part of the attacker to cause

[90] "For example, an intrusion into a military system that has been accredited at Evaluation Assurance Level 7 (EAL7) of the *Common Criteria* is more invasive than openly exploiting vulnerabilities of an openly accessible non-accredited system at a civilian university or a small business." *Tallinn 2.0*, Rule 69, comment 9(d). The *Common Criteria* are standards for independently verifying a computing system's ability to satisfy particular security objectives. Common Criteria, *Common Criteria for Information Technology Security Evaluation*, Part 1: Introduction and General Model, Version 3.1, Revision 5 (April 2017), ¶¶1, 2, 5, accessed October 29, 2019, `https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf`. EAL7 is the highest degree of assurance, certifying that the system ("target of evaluation") has undergone formal design verification, including mathematical proof where necessary, and testing against the owner's security requirements. Common Criteria, *Common Criteria for Information Technology Security Evaluation*, Part 3: Security Access Components, Version 3.1, Revision 5 (April 2017), ¶¶129–132, accessed October 30, 2019, `https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf`. As of 2019, only one such system has been deployed, and that in the Netherlands. Common Criteria, "Certified Products List–Statistics," 2019, accessed October 29, 2019, `https://www.commoncriteriaportal.org/products/stats/`.

[91] One strategy for understanding cyberattacks is to set out what looks to be a vulnerable system and use it to capture data on how attacks progress. These so-called *honeypot* systems are carefully managed to not become a part of the cyberattack, but the activity they record often provides key information about how the attack is managed and can be shut down. Owens report, 148–9, Box 2.4; *Tallinn 2.0*, Rule 32, comment 15; Steve Symanovich, "What Is a Honeypot? How It Can Lure Cyberattackers," NortonLifeLock, May 26, 2020, accessed February 5, 2021, `https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html`.

[92] Austin Davis, "Berlin Gold Coin Heist: 3 Sentenced to Jail," *DW*, February 20, 2020, accessed June 11, 2020, `https://www.dw.com/en/berlin-gold-coin-heist-3-sentenced-to-jail/a-52441680`. The theft occurred on March 27, 2017; three persons were convicted of the theft on February 20, 2020. A recently-hired security guard participated in the theft. At the time of the theft the gold content of the coin was worth about 5.4 times its face value of C$1 million.

an effect inside the target state. Stuxnet (see Chapter 2) took a great deal of planning and was carefully crafted with a single target in mind.[93] Thus it would score highly on the invasiveness criterion if there was also state involvement in its development and deployment (which there was). NotPetya and Sunburst are similarly complex attacks because they first targeted specific software developers and used their build and distribution systems to gain access to the ultimate targets. That degree of effort indicates a high degree of invasiveness with a level of indirection to cover the origin of the attack for long enough to do its damage. Russia's involvement in NotPetya removes any doubt about the intention to be invasive. Sunburst only exfiltrated data, so though it took a great deal of effort to infect its targets, it does not meet the invasiveness criterion, even though it probably will score highly on state involvement by Russia.[94] (Chinese hackers are suspected of exploiting another vulnerability in SolarWind's Orion software, but this is distinct from the Sunburst attack, and as yet there is no evidence of Chinese involvement with Sunburst.[95])

A corollary to the technical complexity of an attack is the human effort required to implement it. This is harder to estimate, but one report of the USA's disruption of *Daesh*'s Internet presence captures some of it.

> [The ARES team] had to build their battle plan from scratch. First they had to map out how ISIS [that is, *Daesh*] operated online—a laborious process in itself—then figure out how to draw the right targets on the map. The deputy chief of Cyber Command, Kevin McLaughlin, who chaired the targeting committee, . . . told the team to constantly ask itself, "What are the types of things that you can do in cyber that actually make a difference to the warfighting side?"
>
> . . .

[93] Zetter, "Stuxnet Missing Link Found, Resolves Some Mysteries Around the Cyberweapon."

[94] Wolfe and Pierson, "Explainer—US Government Hack: Espionage or Act of War?"

[95] Christopher Bing et al., "Exclusive: Suspected Chinese Hackers Used SolarWinds Bug to Spy on 'US Payroll Agency—Sources," *Reuters*, February 2, 2021, accessed February 5, 2021, `https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8`.

> Throughout, the pressure from the top was unrelenting. [Admiral Mike] Rogers "wanted to pull out all the stops to pass this test," a senior official recalls. Even while the effort was weeks old, Pentagon officials began complaining in the press about the slowness of the progress. The crew was working 14-hour days, seven days a week.[96]

The project took a team of between 50 and 100 persons about five months to prepare,[97] so it is not unreasonable to estimate the human effort at 150 thousand hours. This investment in labour is not one a casual or even criminal hacking organization could make. If a cyberattack is precise and complex, it is likely to have had a large research and development organization behind it. The military branches of the most powerful states fall into that category.

These examples illustrate the challenges associated with assessing the *invasiveness* criterion. State involvement, harm to computing systems, the level of system security, some degree of selectivity (discrimination), and the implication of target states' interests are all required for a cyberattack to be considered invasive. *Invasiveness*, as a just-cause criterion, is therefore also connected to *measurability of effects*, *directness*, and *state involvement*.

Presumptive legality

In contrast to the seven other just-cause criteria, *presumptive legality*, if it is found, rules out treating a cyberattack as a use of force. This is a matter of interpreting two principles found in the international law of armed conflict. First, the presumption under international law that activities during an armed conflict are permissible gives wide latitude in what actions a state can take.[98] Second, there are a number of treaties containing clauses which prohibit the use of particular means and methods of warfare or incorporate the Martens clause concerning indefinite proscriptions against acts that deviate from convention, "the laws of humanity, and the public conscience"[99]

[96] Graff, "The Man Who Speaks Softly—and Commands a Big Cyber Army."

[97] Graff.

[98] *Lotus*, ¶¶44–7, cited in *Tallinn 2.0*, Rule 69, comment 9(h).

[99] Hague Peace Conferences, Convention (II) Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, July 29, 1899, preamble, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/

(see Appendix A). Thus not only are there particular constraints on what is permissible during armed conflict, but also imprecise ones that are subject to states' interpretations or fall deep within the "penumbra of uncertainty."

Information warfare and psychological operations fall under this category.[100] The Internet Research Agency (IRA, not to be confused with the Irish Republican Army) based in St. Petersburg, Russia, used social media such as Facebook and Twitter to "denigrate Secretary Clinton . . . [and] to advocate for President-elect Trump as early as December 2015"[101] as part of a larger campaign to influence the electoral process. Further, these "Russian trolls sought to exacerbate tensions over issues such as race, sexual identity and guns."[102] Concurrently, Russia's English-language broadcast and streaming media outlets RT and Sputnik amplified the message that "President-elect Trump [was] the target of unfair coverage from traditional US media outlets that they claimed were subservient to a corrupt political establishment"[103]—in other words, "fake news" fabricated by a "deep state." This contributed to the polarization of American sociopolitical discourse, to the detriment of the state and its people. The cyber aspects of this campaign had state involvement, but no measurable physical effects, and the causal chain in a sociopolitical context is not nearly direct enough to meet that just-cause criterion. Under the *Tallinn Manual*'s criteria, this campaign would fall short of being a use of force against the USA. However, under *presumptive legality,* using cyber and other means to distribute propaganda is not prohibited, and that would also rule out just cause for a use of force in response. This does not mean that the target state has no recourse; it has been

---

OpenAttachment/applic/ihl/ihl.nsf/CD0F6C83F96FB459C12563CD002D66A1/FULLTEXT/IHL-10-EN.pdf (hereafter cited as HC II (1899) Annex).

[100] *Tallinn 2.0*, Rule 69, comment 9(h).

[101] Office of the Director of National Intelligence [USA], *Assessing Russian Activities and Intentions in Recent US Elections*, intelligence community assessment, ICA 2017-01D, January 6, 2017, 4, accessed February 5, 2021, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[102] Ellen Nakashima, "US Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, accessed February 4, 2021, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

[103] Office of the Director of National Intelligence [USA], *Assessing Russian Activities and Intentions in Recent US Elections*, 4.

reliably but unofficially reported that US Cyber Command "basically took the IRA offline" during the USA's 2018 elections[104] by similarly permissible cyber means.

Presumptive legality is also extended to most cases of espionage,[105] though there is dispute over the extent to which espionage by cyber means violates a state's sovereignty.[106] This disagreement is a fine point that makes little practical difference with respect to providing just cause under *jus ad bellum*.

On the one hand, assuming that espionage (either by traditional or by cyber means) is a violation of sovereignty, that by itself would not be cause for an armed response unless some degree of harm satisfying the other just-cause criteria had occurred in the act of collecting and exfiltrating information. But then it is the harm that provides just cause, not the act of espionage itself. However, as a violation of sovereignty, and thus a breach of an international obligation on the part of the state doing the espionage, the limits on countermeasures restrict the response to one where "there is no patent imbalance between the underlying wrongful act and the countermeasure."[107] In the case of a person doing the spying, an appropriate countermeasure is to arrest the spy and lodge a diplomatic complaint, not bomb an airfield. In the case of cyber espionage, that means taking steps to neutralize the malware and pursuing a diplomatic complaint. The act of espionage by itself justifies countermeasures, but is not just cause for an armed response. On the other hand, if espionage is not considered a violation of sovereignty, then the domestic laws of the target state apply with respect to the spying (perhaps with extraterritorial complications in the case of cyber espionage[108]), unless any physical harm caused while carrying out the espionage constitutes a violation of sovereignty. Again, it is this harm that would provide just cause for an armed response, provided the relevant criteria are met. The question of espionage as a violation of sovereignty makes no difference in this regard.

Traditional means of espionage require having an agent physically present in the target state's territory.[109] Espionage by cyber means does not require

[104] Nakashima, "US Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms."

[105] *Tallinn 2.0*, Rule 69, comment 9(h).

[106] *Tallinn 2.0*, Rule 4, comments 7, 8.

[107] *Tallinn 2.0*, Rule 23, comment 5.

[108] *Tallinn 2.0*, Rule 32, comment 17.

[109] *Tallinn 2.0*, Rule 4, comments 7, 8; Rule 32, comment 9.

an agent to be present in the target state.[110] If the cyber espionage is conducted remotely, then the act of espionage itself will not directly violate state sovereignty.[111] This means that cyberattacks like Sunburst, when they infect and exfiltrate data from US government departments[112] to their originating states, are not in breach of an international obligation unless and until they cause some other harm that does.[113] Since Sunburst is not yet known to have done anything more than extract and transmit sensitive data from infected systems, it is being treated as an act of cyber espionage,[114] not an act of cyberwarfare, and thus not just cause for a use of force against the originating state.

Even though espionage is a widely accepted practice among states (and there would be a significant strategic disadvantage to eschewing the practice on a unilateral basis), there are no agreed limits on the content of the information gathered, and very few on how that information may be used. In the context of the laws of armed conflict, espionage can give a state valuable information that facilitates distinguishing between military and civilian targets or determining what actions would be proportionate to any threat or objective. It may also clarify intentions with respect to activity that looks like a threat but is really a simulation exercise. These outcomes minimize harm. However, espionage can also feed a confirmation bias for the belief that an attack is imminent when none is planned. But espionage (broadly construed) is not yet limited to strictly military or foreign policy purposes, even in the absence of armed conflict.[115] The "war" on terror has been used to justify extending espionage to a practice that approaches warrantless surveillance of domestic and foreign civilians.[116] The open and international char-

[110] *Tallinn 2.0*, Rule 32, comment 4.

[111] *Tallinn 2.0*, Rule 32, comment 6.

[112] Zachary Cohen, Vivian Salama, and Brian Fung, "US Officials Scramble to Deal With Suspected Russian Hack of Government Agencies," *CNN Politics*, December 14, 2020, accessed February 6, 2021, https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia; Fung, "Why the US Government Hack Is Literally Keeping Security Experts Awake At Night."

[113] *Tallinn 2.0*, Rule 32, comment 6.

[114] Wolfe and Pierson, "Explainer—US Government Hack: Espionage or Act of War?"

[115] *Tallinn 2.0*, Rule 4, comment 27.

[116] Adam M. Segal, "Cyberspace: The New Strategic Realm in US-China Relations," *Strategic Analysis* 38, no. 4 (July 2014): 578–80, https://doi.org/10.1080/09700161.2014.918447.

acter of Internet and telephony services makes cyber surveillance (as an extreme form of espionage) a tempting opportunity for states to cast the data-harvesting net too broadly in the search for threat intelligence.

While terrorism and international criminal activity do impinge on state interests, they are not the kind of thing that the laws of armed conflict control. They are explicitly excluded from being considered as an international armed conflict. Though there is good reason to tacitly permit the practice of espionage by not prohibiting it under international law, it would be better to explicitly permit espionage for military purposes (whether it supports finding a just cause in the *jus ad bellum* context, or attaining a legitimate military objective or reducing potential civilian harm in the *jus in bello* context) and perhaps broader foreign policy purposes. This permission should not be broad enough to allow widespread warrantless surveillance of individuals—a violation of the right to freedom from "arbitrary or unlawful interference with his privacy, family, home, or correspondence"[117] for persons within a state bound by ICCPR.

Finally, *presumptive legality* is accorded to coercive economic disruption. There is no acceptance by the broad international community that the disruption of another state's economy by cyber means is a violation of state sovereignty, and therefore a violation of international peace and security. This is consistent with the idea that economic sanctions against a state do not by themselves constitute a use of armed force.[118] The only way an economic disruption caused by cyber means might justify an armed response is if the civilian population suffers immediate life-threatening harm as a result. So, in the absence of other harms, invasive actions for economic disruption do not provide just cause for a forceful response. They are presumptively

[117] ICCPR, Art. 17.

[118] UN Charter, Art. 41; *Tallinn 2.0*, Rule 69, comment 2. The ineffectiveness of economic sanctions in promoting policy change, the disproportionate and indiscriminate effects on civilians (in violation of the principle of distinction; Albert C. Pierce, "Just War Principles and Economic Sanctions," *Ethics and International Affairs* 10 (March 1996): 99–113, https://doi.org/10.1111/j.1747-7093.1996.tb00005.x), the growing recognition that economic inequity does pose a threat to peace and security, and the asymmetry of power (in that sanctions are a measure that only large, wealthy states have the means to wield, and that only against smaller, poorer ones) provide cause for rethinking this position. However, the *Tallinn Manual* deals with international law as it stands, not as we might want it to be. *Tallinn 2.0*, Rule 4, comment 28. While this is a fascinating and complex topic in itself, further discussion is out of scope for this project.

legal in the context of international law because they are not explicitly prohibited,[119] though some states are starting to rethink this position. In particular, the USA has reserved for its president "the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyberattacks directed against the US economy. . . . "[120] The difficulty comes in characterizing *significance*. If the aggressive cyberoperation's economic effects proximally cause civilian harms proscribed by international law, there may be cause for a lawful armed response. However, the disruption of stock, bond, and derivative markets (by any means, not just cyber means) is not the kind of harm the laws of armed conflict anticipated being taken as just cause for such a response. In other words, as international law currently stands, it is presumptively lawful for a state to wreak this kind of financial harm against those who have the means to participate in those markets.

Departures from just-war theory

The international laws of armed conflict do not incorporate two requirements of just-war theory's *jus ad bellum*: *right intention* and *probability of success*.[121] The *Tallinn Manual*, as an interpretation of existing international law, inherits and preserves these shortcomings, with some reason. The first concern, *right intention*, reflects a broader evidential (and thus epistemological) problem with respect to discerning intent in a reliable way.[122] While a state's intention may seem clear by its actions, gathering the documentary evidence to prove its intention is a *post bellum* endeavour simply because access to secret state records and facilities will not be available to adjudicators during the conflict. Moreover, right intention does not have to be demonstrated

[119] *Tallinn 2.0*, Rule 69, comment 9(h).

[120] Department of Defense [USA], *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, technical report (November 2011), 4, accessed February 10, 2021, https://www.acqnotes.com/Attachments/DoD%20Cyberspace%20Policy%20Report%20A%20Report%20to%20Congress%20Pursuant%20to%20the%20NDA%20Act%20Nov2011.pdf; David Alexander, "US Reserves Right to Meet Cyber Attack With Force," *Reuters*, November 15, 2011, accessed February 10, 2021, https://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116.

[121] Orend, "War," §2.1.

[122] Orend, §2.1.

by the target state in determining whether it has just cause to respond to an attack in self-defence. Once a state has been subject to an armed attack, it has that just cause. Setting out when a state may be justified in making the first strike in an armed conflict is beyond the scope of the *Tallinn Manual*. Rather, it presumes, in accordance with the UN Charter, that a state would not contemplate being the initiator of an international armed conflict, only a responder to another nation's unlawful first strike.

The second, *probability of success*, tilts the balance of any conflict in favour of states with more resources. This would preclude smaller or less powerful states from initiating an armed conflict against larger or stronger states, denying them some of their rights as states in the international community,[123] such as the "sovereign equality of States."[124] Again, the *Tallinn Manual* does not err in being silent on this matter, since it does not contemplate being the initiator of an armed conflict by cyber means. However, the apparent cost asymmetry of cyberwarfare, with the cost and resources required to launch a cyberattack usually being much lower than the cost and resources required to defend against one, may reduce this imbalance and increase the probability of a smaller state succeeding in its objective against a larger one—provided the conflict remains strictly within the cyber realm. The emergence of cyberwar may make this just-war criterion economically feasible to smaller states, and thus more accessible to them.

4.4 The *Tallinn Manual* and *jus post bellum*

Jus post bellum in international law

The idea of *jus post bellum*, or the just conclusion of a war in order to establish a just peace, is a relatively recent development in just-war theory. Brian Orend notes that international law has not yet developed to incorporate much of this dimension of just-war theory, but that there are still some moral considerations that can inform the process of ending a war in a way that promotes justice.[125] These principles are set out in Table 2.3.

[123] Orend, §2.1.

[124] United Nations, "What We Do," December 18, 2018, accessed October 2, 2019, `https://www.un.org/en/sections/what-we-do/`.

[125] Orend, "War," §2.3.

International humanitarian law touches on some of these considerations without couching them in terms of just-war theory. The principle of *restitution* for violations of an agreed convention is first set out in HC IV (1907): "A belligerent party which violates the provisions of the said Regulations shall, if the case demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces."[126] This has been extended to apply to the state responsible for the violation, regardless of who committed it.[127] However, this does not go as far as making reparations for the damage caused throughout the entirety of the conflict.

The principle of *just punishment* for war crimes is set out in GC I–IV (1949), which all include articles prescribing "effective penal sanctions for persons committing, or ordering to be committed, any of the grave breaches of the present Convention."[128] These "grave breaches" are identified as "wilful killing, torture or inhuman treatment, including biological experiments, wilfully causing great suffering or serious injury to body or health,"[129] "extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly,"[130] "compelling a prisoner of war to serve in the forces of the hostile Power, or wilfully depriving a prisoner of war of the rights of fair and regular trial,"[131] "unlawful deportation or transfer or unlawful confinement of a protected person, [and] taking of hostages."[132] All of these are prohibited under the *jus in bello* aspects of international law, and so fall under the rubric of war crimes that must be prosecuted as part of *jus post bellum*.[133] The criminal responsibility for a war crime always attaches to individual persons, whether they be following orders or giving them, either as a military officer or a civilian (government official) with the authority to direct military activity,[134] and states must pros-

[126] HC IV (1907), Art. 3.

[127] International Committee of the Red Cross (ICRC), *Rules*, Rules 149, 150.

[128] GC I, Art. 49; GC II, Art. 50; GC III, Art. 129; GC IV, Art. 146.

[129] GC I, Art. 50; GC II, Art. 51; GC III, Art. 130; GC IV, Art. 147.

[130] GC I, Art. 50; GC II, Art. 51; GC IV, Art. 147.

[131] GC III, Art. 130; GC IV, Art. 147 says the same with respect to "a protected person," meaning a civilian, and with an indefinite article before "hostile Power."

[132] GC IV, Art. 147.

[133] International Committee of the Red Cross (ICRC), *Rules*, Rule 156 describes other violations of international law's *jus in bello* as war crimes that must also be prosecuted.

[134] International Committee of the Red Cross (ICRC), Rules 151–153.

ecute these war crimes.[135] The principle of *discrimination* means that ordinary civilians are not subject to punishment (individually or collectively) for war crimes, just as the corresponding *jus in bello* principle extends nominal protection from being lawful targets during an armed conflict.[136]

GC IV also makes a nod in the direction of the *vindication of rights* with respect to life, liberty, and property, obliging parties to cancel "restrictive measures taken regarding protected [alien] persons . . . [and] their property . . . as soon as possible after the close of hostilities."[137] Later developments grant the right to return to any displaced persons and protection individual property rights,[138] though neither articulation goes as far as vindicating the "community entitlements to territory and sovereignty"[139] that may have been violated either in the lead-up to the conflict or during the course of it. The principles of *proportionality*, *public proclamation*, and *rehabilitation* toward a minimally just society are not part of general international law, but should be a part of the treaty ending the armed conflict (which then becomes international law for the parties involved).

Cyber *jus post bellum*

The *Tallinn Manual* makes no explicit mention of vindication of rights *post bellum*, though, as noted in Chapter 3, it does assert the application of human rights in the cyber realm.[140] Any vindication of rights would include access to and privacy in activities conducted in cyberspace where the technology is available.[141] A state is obliged to make reparations for harm caused by "an internationally wrongful act committed by cyber means,"[142] though the consensus is that the cost of reparations extends only to "material damage . . . when said harm can be assessed in financial terms."[143] This includes "interference with cyber operations or the loss of data that results in finan-

[135] International Committee of the Red Cross (ICRC), Rule 158.

[136] Orend, "War," §2.3.

[137] GC IV, Art. 46.

[138] International Committee of the Red Cross (ICRC), *Rules*, Rules 132, 133.

[139] Orend, "War," §2.3.

[140] *Tallinn 2.0*, Rule 34, comment 1.

[141] *Tallinn 2.0*, Rule 35, though comment 6 to the rule holds that privacy is not an absolute right and may be subject to limitations.

[142] *Tallinn 2.0*, Rule 28.

[143] *Tallinn 2.0*, Rule 28, comment 2.

cial loss."[144] Even so, there is still no consensus about the status of data as property that merits the protection and compensation that tangible private property does.[145] In addressing war crimes committed by cyber means, the *Tallinn Manual* is in accord with GC I–IV (1949) and other conventions set out in Rule 156 of *Customary International Humanitarian Law*,[146] with civilians,[147] commanders, and government officials[148] all liable to individual prosecution for committing war crimes. The *Tallinn Manual*, as an interpretation of existing international law, does not seek to address the requirements of *jus post bellum* that international law does not already address, and so provides no real guidance in terms of ending an armed conflict in a just manner.

4.5 Conclusion

It is fair to conclude that while the rules in the *Tallinn Manual* do not fully satisfy the criteria, obligations, and requirements of just-war theory, it does no worse in this regard than the larger body of international law does. By identifying plausible criteria for assessing the *jus ad bellum* condition of just cause, the *Tallinn Manual* includes more of international law than other domain-specific manuals do. This is valuable because it gives insight into how difficult the determination of just cause for a use of force is. Further, the *Tallinn Manual*'s assertion that at least some human rights apply in cyberspace makes protecting these rights an aspect of *jus post bellum* that must be addressed in any just post-conflict resolution.

While the application of the laws of armed conflict to the cyber realm is enough to make the *Tallinn Manual* an important contribution to international law, the discussion of just-cause conditions under *jus ad bellum* and the explicit consideration of human rights treaties set a new standard for

[144] *Tallinn 2.0*, Rule 28, comment 2.

[145] *Tallinn 2.0*, Rule 149, comment 3. This uncertainty is expressed in the context of occupation of another state's territory. If data does not have protected status within occupied territory, even when the occupation is conducted in accordance with the laws of armed conflict, its loss is not currently seen as a compensable harm. Following this reasoning, loss of data through any violation of the law of armed conflict during would not likely be compensable.

[146] *Tallinn 2.0*, Rule 84.

[147] *Tallinn 2.0*, Rule 84, comment 3.

[148] *Tallinn 2.0*, Rule 85.

domain-specific manuals. As such, the *Tallinn Manual* should be included among the authoritative presentations of international law, and its findings—particularly the ones where the agreement was only to the wording of the rule and not its interpretation—given attention in matters concerning international law in the cyber realm, particularly as they approach the ideals of just-war theory. I turn now to two specific difficulties the *Tallinn Manual* has identified in the just-cause criteria of *jus ad bellum*.

Chapter 5

Cyber *jus ad bellum*: the problems of scale and effects

5.1 Cyberharms in meatspace

When one state makes an armed attack against another state by conventional means such as bombs and projectiles, the attack has immediate effects over a definable area. Biological and nuclear weapons produce longer-lasting effects over wider areas. While the physical damage produced by a nuclear weapon is an immediate effect, the radioactive fallout continues to cause harm for a much longer period of time. The first signs of harm from a biological attack, however, may take days or weeks to emerge, and because of human mobility, may emerge far from the site of the initial attack. Thus there can be temporal and geographical gaps between the attack and the awareness that an armed attack has taken place, and a much longer temporal gap before knowing the full scale and effects of the attack. With respect to cyberattacks, there may be a greater causal distance (in terms of number of discrete events) between the initiation of the cyberattack and its effects. This chapter addresses some of the problems that come with assessing the just-cause criteria of *severity*, *measurability of effects*, *immediacy*, and *directness*, and introduces ways of classifying cyberattacks and permissible responses with respect to these criteria.

It is easy to think that with the speed of digital communication and continually increasing computational efficiency (at least with respect to clock time), cyberattacks would typically be short-lived events with immediately

visible results and few ongoing consequences with respect to the physical world—something analogous to conventional explosive devices. For example, a downloaded malicious program such as WannaCry that encrypts all of a computer's files is a cyberattack with a short attack phase and immediate effects. A simple *logic bomb*, a piece of malicious code running undetected on a computing device, waits for a trigger before "going off," producing its intended harm on that device. This kind of cyberattack is analogous to conventional sea or land mines.[1] Unlike conventional, biological, or nuclear weapons, these kinds of cyberattacks will not cause direct physical harm to humans.

However, more sophisticated cyberattacks can have attack-to-effect patterns that look more like those of nuclear or biological weapons, including causing harm to humans. Some logic bombs can induce cascading software and hardware failures that eventually result in significant physical damage and civilian deaths. While this physical damage may be the primary goal of such a cyberoperation, the event that finally produces that damage may be temporally, causally, and geographically distant from the original placement of the logic bomb. The stealthy spread of malicious software is similar to the spread of a virus with a long latency or incubation period before the effects begin to show. And while a cyberattack does not (directly) produce widespread fallout, it can be as disruptive to computing equipment as the electromagnetic pulse from a nuclear detonation is. Further, a well-executed cyberattack can have damaging psychological effects with respect to security of the state and disruption of society, just as nuclear and biological attacks would. These psychological effects are often geographically removed from the location of any physical damage.

The Cold War between the USA and the USSR during the mid- and late 1900s provides a vivid, though unofficial, account of such a cyberoperation. In 1982 a natural gas pipeline in Siberia was allegedly damaged by a cyberattack. The USSR was aiming to sell natural gas to states in western Europe in order to get "hard" Western currency. As the story goes, they needed software to control and monitor the flow of gas through a new pipeline running from Siberia to the border with the West. No American company was willing to make the sale, so the Soviets had to get creative. American intel-

[1]The similarity to mines would be clearer if these were called *cyber mines*, but *logic bomb* is the common term for this kind of malicious software.

ligence officials uncovered the exfiltration of control software from a Canadian control systems specialist, and they informed the developer that there was reason to believe the USSR was behind it. The developer quickly devised a logic bomb, inserted it in the code, and left it for the Soviets to retrieve and install.[2] Some time later, the pipeline burst.

While this cyberoperation's goal was to disrupt the USSR's economy by preventing the sale of natural gas to western Europe,[3] the cyberattack directly targeted only the pipeline's control system; the explosion itself was considered an indirect effect of the cyberattack.[4] Further, while destroying part of the pipeline provided a temporary physical impediment to transporting natural gas westward, the greater disruption was psychological: even if the pipeline could be repaired and the relevant control systems replaced, there was no longer any certainty about the reliability of other pirated software.[5] Regaining trust in the control systems would take more time than just repairing the pipeline did. The USSR had to balance the risk of further harm against the need to make money that could be spent in the global marketplace. This longer-lasting and more distant indirect effect was the intended outcome.[6] The software-facilitated explosion was the means to that economic end.[7]

Assessing the harm resulting from an aggressive cyberoperation is more complex than in conventional or nuclear warfare. However, the resolutions of the international community, interpreted in a cyber context, do offer

[2]Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York, NY: Ballantine Books, 2005), 268–69.

[3]Owens report, 195.

[4]Owens report, 113. Thomas Reed described the explosion as "the most monumental non-nuclear explosion and fire ever seen from space. . . . The Air Force chief of intelligence rated it at three kilotons . . . " Reed, *At the Abyss*, 269. There are no official reports of anyone being killed in the explosion, though any workers near the burst almost certainly would have been killed.

[5]Reed, 269.

[6]Reed, 269.

[7]There is some evidence to suggest that the story may a confabulation of Central Intelligence Agency (CIA) Cold War strategies and an accidental explosion along the pipeline. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 10–11, https://doi.org/10.1080/01402390.2011.608939. The Owens report, 195, also refers to the incident as an alleged cyberattack, but the involvement of Admiral Owens, former Vice Chairman of the Joint Chiefs of Staff, in preparing the report lends some credibility to Reed's account.

some guidance when deciding whether such aggressive cyberoperations have become equivalent to an armed attack carried out by conventional means: identify and assess the *scale and effects* of the harm done.[8] But the distances—geographic, temporal, and causal—from the deployment of a logic bomb and its destructive effects complicates this judgement. One example of this is the Stuxnet worm, which has significant distance in all three of these aspects. Stuxnet damaged equipment at an Iranian uranium-enriching facility in 2010, but the worm could not be installed directly by the parties wanting to disrupt Iran's nuclear program. Instead, the worm was set loose on the public Internet and relied on both Microsoft Windows' software vulnerabilities and benign human activity to cross into the private network within the facility. An employee unknowingly brought the worm across the so-called *air gap* between the public Internet and the private network by attaching an infected USB storage device to a computer on the internal network. From there the worm could finally find its way to its intended targets—the controllers for the centrifuges used to separate different isotopes of uranium.[9]

[8] *Nicaragua Judgement*, ¶195, introduces this terminology, but it refers to United Nations General Assembly, "Definition of Aggression." Article 3(b) of the UN General Assembly resolution declares that "the use of any weapons by a State against the territory of another State" qualifies (*ceteris paribus* under Article 2) as an act of aggression, and Article 4 points out that the Security Council ultimately determines which actions, once committed, are aggressive. The ICJ ruling gives some clarifying language around how this determination can be made, but it does not set out specific thresholds, and its ruling only carries full legal weight with respect to the case at hand. The 2010 amendment to the Rome Statute of the International Criminal Court incorporates Article 3(a)–(g) of the UN General Assembly's definition in its entirety as crimes of aggression. International Criminal Court (ICC), Rome Statute of the International Criminal Court, 2011, 2187 UNTS 90, amended, The Hague, NL, Art. 8 *bis* (2), accessed April 8, 2020, https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf. By the end of 2020 this amendment to the Rome Statute had been recognized by only 40 states, none of them permanent members of the UN Security Council. However, the UN General Assembly's definition, taken together with the ICJ's acceptance of that definition, suggest the presence of some official support for labelling the particular actions described there as acts of aggression under international law regardless of states' reluctance to accept the Rome Statute amendment.

[9] Stuxnet had also been found on computers at the Bushehr nuclear power plant, suggesting that the reactor was the target. Ryan Paul, "Iranian Power Plant Infected by Stuxnet, Allegedly Undamaged," *Ars Technica*, September 27, 2010, accessed November 23, 2020, https://arstechnica.com/information-technology/2010/09/iranian-power-plant-infected-by-stuxnet-allegedly-undamaged/. Later research would show that the

It was ultimately determined that the actual harm and potential harm of the Stuxnet attack, even though it was a clear violation of Iran's sovereignty, did not, and was not likely to, reach an equivalent to the level of an armed attack.

If there is a complex chain of (macro-scale) events between an aggressive cyberoperation and its ultimate effects, it is harder for the target state to claim that the act of deploying malicious code by itself is a use of force rising to the level of an armed attack. Even though the scale and effects of that cyberoperation and subsequent events could support such a claim,[10] determining what role the cyberoperation itself played may affect the justification of the claim. Similarly, some aggressive cyberoperations may be intended to produce effects at a distant location at an indeterminate time in the future through a causally short and relatively direct, but temporally prolonged, set of events. But these kinds of cyberoperations are more easily disrupted than ones producing an immediate effect. While the *Tallinn Manual* suggests that if a mere inconvenience results, the cyberoperation is not a use of force justifying an armed response,[11] it also suggests that if the likely results would have been equivalent to a use of force by conventional means, it could be argued counterfactually that the failed or thwarted cyberoperation could be deemed a use of force because of the intention to cause harm.[12] For example, if Stuxnet had caused a release of radioactive material from the centrifuges, or if it had targeted the nuclear reactor at Bushehr instead of merely infecting machines that controlled a reactor as it searched for the centrifuges, then both the real effects in the former case and the potential nuclear disaster in the second would give reason to claim that the harm, whether actual or intended, would have been equivalent to the effects of an armed attack targeting the enrichment or reactor sites.

---

facility supplying uranium for the reactor was the target, and not the reactor itself. Mark Clayton, "How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant," *Christian Science Monitor*, November 16, 2010, accessed February 15, 2021, https://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant; Farwell and Rohozinski, "Stuxnet and the Future of Cyber War," 24; Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons," 81–2, 85. Regardless, it was a strike against Iran's nuclear program, and that aspect of Stuxnet is taken up in Chapter 2.

[10] *Tallinn 2.0*, Rule 69, comment 9(c).

[11] *Tallinn 2.0*, Rule 69, comment 9(a).

[12] *Tallinn 2.0*, Rule 92, comments 16, 17.

5.2 Moderate and flagrant cyberattacks

As the pipeline example shows, the assessment of the scale and effects of any aggressive act is multifaceted. There will be cases that seem easy to assess, such as the loss of a few hundred civilian lives in a factory making armoured vehicles or the sudden shutdown of a research assistant's laptop computer in a military research lab. The difficult cases fall somewhere in between. Yet even those apparently clear scenarios will have confounds. Not only is there no bright line dividing aggressive actions that are clearly equivalent to an armed attack and those that are not; there are also no bright lines to bound a messy middle ground. Any assessment will unavoidably be coloured by the epistemic state of each party involved in the action and the relative priority each party gives to the different criteria for assessing the severity of effects.

Development of effects

The Owens report identifies four significant time periods that are relevant to aggressive cyberoperations.

> . . . $T_{\textit{intelligence collection}}[]$ is the period available for collecting intelligence needed to launch the attack. . . . $T_{\textit{attack launch}}[]$ is the period over which the functionality required to carry out the attack on the targeted system(s) is installed or deployed—that is, during which the attack is launched. . . . $T_{\textit{compromise}}[]$ is the period over which the confidentiality, integrity, or availability attributes of the targeted system(s) are compromised. . . . $T_{\textit{effects apparent}}[]$ is the time period over which the victim actually suffers the ill effects of such compromises. . . . Depending on the specific nature of the cyberattack, these four periods may—or may not—overlap with each other.[13]

These time periods provide a point of reference for treating cyberattacks analogously to conventional ones. I show the relationships between them in diagrammatic form in Figure 5.1.

[13] Owens report, 89–90. These time periods, illustrated in 'Figure 5.1'=latex, have counterparts in the planning and execution of any response the target state may choose to make, as illustrated in 'Figure 5.2'=latex.

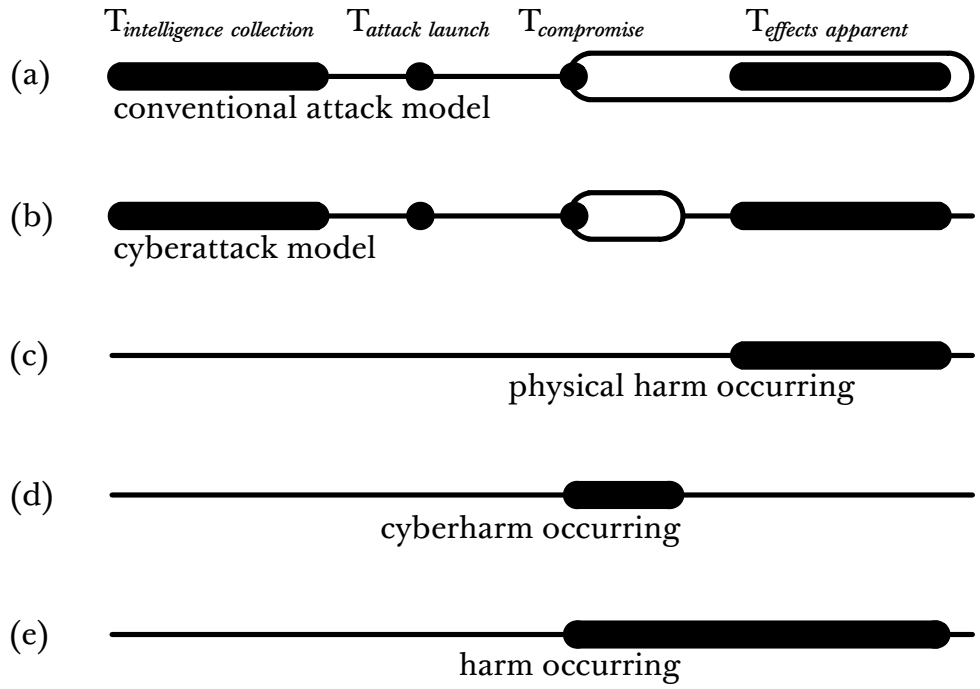


Figure 5.1: Owens report schematic timeline. Timelines (a) and (b) show the order of significant events described in the Owens report.[a] Solid markers indicate the distinct events under this schema, and open markers indicate the time period when the target is compromised by the attack. The timeline shows the order of events and not the amount of time between them. Timeline (a) illustrates the model of a conventional attack, where the time periods of vulnerability to attack and of suffering effects overlap. Timeline (b) illustrates the model of a cyberattack, where the target system needs only to be compromised at some time before the effects become apparent. The cyberattack can be withdrawn before, during, or after the effects manifest. Timeline (c) shows the period of time when physical harm is occurring, from the point in time where the physical effects are first apparent to the point in time when the immediate physical effects end. Timeline (d) shows the period of time when cyberharm is occurring, from the point in time where the target system is compromised to the point in time where the cyberattack ends or is withdrawn. Timeline (e) shows the period of time when harm is occurring if harm is understood as being inflicted as soon as the target is compromised, and ending at the later of the ends of $T_{compromise}$ and $T_{effects\ apparent}$, reflecting the full duration of cyber and physical harm resulting from a cyberattack.

[a] Owens report, 89–90.

All of these time periods are also relevant to attacks made by conventional means. For example, $T_{attack\ launch}$ in the context of a conventional attack is the beginning of the physical phase of the attack such as the launching of cruise missiles, sending out a sortie for aerial bombardment, or blockading a port. $T_{compromise}$, the time at which the target state is compromised, occurs once the border has been breached by the attacker—that is, the target state's integrity has been violated. The attacking state is now in a position to do physical damage, but may still hold off on producing that damage (Figure 5.1(a)). Similarly, an attacking state can leave a compromised computer operating in an apparently normal fashion until the time when it activates the harm-producing part of the cyberattack. The appearance of those downstream effects may come after the target system has been restored to normal operation and is no longer vulnerable itself (Figure 5.1(b)). The beginning of $T_{compromise}$, then, marks the point in time when everything is in place to execute the strike. Regardless of the means of the attack, $T_{effects\ apparent}$ begins when the first of the effects becomes apparent.

This time-period framework offers a starting point for grappling with the conjoint matters of scale and effects. An argument could be made that, at least in the case of an aggressive cyberoperation, deleterious effects begin not with the emergence of physical harm at $T_{effects\ apparent}$ but at the point of system compromise, the beginning of $T_{compromise}$ (Figure 5.1(e)). After that point, even though the operation of the target system may appear normal, the data managed by the system is no longer confidential, the integrity of operational data is no longer guaranteed, and the periodic, rarely-used functions of the system may not be available.[14] For example, the modified software could intercept a shutdown command for a particular machine and transmit a series of signals designed to break the machine, but report to the operator that the shutdown had completed successfully. Inducing the mechanical failure marks the beginning of $T_{effects\ apparent}$ on the given account, but the direct effect of the cyberoperation, the precursor to the intended one, began at $T_{compromise}$, when this effect was not apparent to the target state.

The UN General Assembly's definition of aggression gives limited support to the view that $T_{compromise}$ is the point where it can be considered that an aggressive action has taken place. An invasion without any further physical

[14] Owens report, 90.

harm is almost always going to be considered an act of aggression.[15] Compromising the operation of a military computing system may just be physical enough (with respect to the physical representation of data and code in electromagnetic form) that it can be considered an invasion—provided the malware was installed under the direction of the attacking state's armed forces. This satisfies the just-cause criteria of invasiveness, state involvement, and military character, but not necessarily the other criteria of severity, measurability of effects, immediacy, and directness identified in Table 4.1. At this point a response of some sort is justified. However, if no damaging attack follows the invasion or compromise, then the same resolution that defines aggression also grants the UN Security Council the ability to "conclude that the determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity."[16] In other words, even if $T_{compromise}$ is the point when a military operation has become an act of aggression, if more serious effects do not occur (so $T_{effects\ apparent}$ is never reached), it is difficult to justify calling the preliminary stages anything more than a threat rather than an armed attack. The target state has to justify any response stronger than what is required to end the threat. If that planned response is a use of force, that justification must address all of the *jus ad bellum* conditions, and not only the remaining just-cause criteria.

An analogous conventional attack serves to illustrate this point. The mere compromise of a computing system, as serious as it is, is no more an act of war than a short-lived border skirmish is. Yet a border skirmish can cause more physical damage than the compromise of a computer system. In this regard, then, any claim that merely compromising a computing system is a greater threat to a state's sovereignty or does greater harm than a border skirmish is difficult to sustain. But a "mere frontier incident"[17] is not, on its own, an armed attack. Unless and until significant damage results from disrupting the normal operation of a computing system, effects comparable to those arising from a conventional armed attack have not occurred—in other words, the result of assessing severity using the criterion of physical harm are exactly the same for small-scale cyber and conventional attacks:

[15] United Nations General Assembly, "Definition of Aggression," Art. 3(a).

[16] United Nations General Assembly, Art. 2.

[17] *Nicaragua Judgement*, ¶195.

where there are no significant and lasting physical harms to be found, there is no just cause for a use of force in response.

Extent of the effects

Assessing the scale and effects of a particular aggressive cyberoperation against a state is typically a qualitative judgement: how similar and how widespread is the harm resulting from that action to any historical actions, regardless of means, that have been deemed to be armed attacks?[18] If the aggressive cyberoperation meets that vague comparative threshold, then (assuming the other just-cause criteria and *jus ad bellum* conditions are satisfied) the target state is permitted to act in self-defence[19] using whatever means are necessary and proportionate to the military goal of ending the threat against it.[20] If a cyber response satisfies the *jus in bello* obligations and will have less severe effects than a response by conventional means, it is to be preferred. If a cyber response is not sufficient to end the threat, a limited conventional response may be permissible; however, any conventional response risks escalating the conflict by extending it into meatspace (and perhaps failing the *jus ad bellum* condition of proportionality where the harm outweighs the global benefit). If non-forceful means like diplomatic protestations will end the threat, then a forceful response, either cyber or conventional, is not necessary and is therefore not permitted.

Though all state-involved cyberattacks are attempts to violate another state's sovereignty in some way, state-involved cyberattacks are not of equal consequence. This suggests classifying aggressive cyberoperations into two categories with a messy middle:[21] *moderate* cyberattacks that are more annoying or irritating than harmful, and *flagrant* cyberattacks that deliberately and maliciously "impinge on critical national interests."[22] Of course, these national interests may be impacted to a greater or lesser degree by any par-

[18] *Tallinn 2.0*, Rule 69; Rule 71, comments 6, 7.

[19] UN Charter, Art. 51.

[20] *Tallinn 2.0*, Rule 72, comment 5.

[21] I thank Brian Orend for his helpful suggestion of a *thick/thin* division of cyberattacks. *Flagrant* captures the intention and intensity of a cyberattack in the thick sense, while *moderate* reflects the non-trivial but comparatively mild and localized impact of a cyberattack in a thin sense.

[22] *Tallinn 2.0*, Rule 69, comment 9(a).

ticular cyberattack, but one of the goals of the *Tallinn Manual* is to provide guidance for determining when a cyberattack is a flagrant violation of international norms while shrinking the conceptual messy middle as far as the collective will of the international community permits. Flagrant cyberattacks may provide just cause for a use of force in response provided the other just-cause criteria are met; moderate ones will not. Corresponding to these are the different categories of permissible responses: *non-forceful* (or, in the language of the UN Charter, *pacific*[23]), *moderate* cyber responses that will not cause physical damage, and *nocuous* cyber or conventional responses that are likely or intended to cause physical harm. Conventional responses to cyberattacks will target physical infrastructure with the intention to damage them, so they cannot fall into the *moderate* category.

If classifying a cyberattack depends on how it affects critical national interests, it helps to give some shape to what those interests are. The idea of *critical national interests* derives from a state's sovereignty over its territory and its exercise of "inherently governmental functions."[24] Territorial sovereignty extends to persons, objects, and property within that territory, including cyber infrastructure within that territory, regardless of who owns it[25] (with limited exceptions for diplomatic purposes). It also extends to the activity that is carried out within that infrastructure,[26] whether it is government activity or private activity. It is possible, then, for a state to violate another state's sovereignty through its activity in that second state's cyber infrastructure.[27] The idea of *inherently governmental functions* includes honouring its international obligations (including its international human rights obligations[28]) and the means by which a state facilitates its "political, social, cultural, economic, and legal order."[29] (Matters of foreign policy, national security, and the armed forces fall most cleanly under the political function of the state, but they can also be associated with the other broad functions.) Disrupting any of these functions without the resolution of the UN Security Council is very likely to be a violation of the state's sovereignty, just as a territorial

[23] UN Charter, Ch. 6.

[24] *Tallinn 2.0*, Rule 4, comment 10.

[25] *Tallinn 2.0*, Rule 1, comment 4; Rule 2, comments 3, 4, 6; Rule 4, comment 5.

[26] *Tallinn 2.0*, Rule 2, comment 7.

[27] *Tallinn 2.0*, Rule 4, comment 1.

[28] *Tallinn 2.0*, Rule 2, comment 8; Rule 35.

[29] *Tallinn 2.0*, Rule 2, comment 10.

violation would be.[30]

One consideration is whether an act of aggression has consequences severe enough for the action to be viewed as a use of force. Aggressive acts that result in "physical harm to individuals or property" are clearly uses of force,[31] but where no such harm is apparent, then this determination becomes more difficult. Michael Schmitt's initial formulation of this criterion suggested the impact on human well-being (and in particular the hierarchy of needs) be a guide to assessing severity.[32] The more basic the need that can no longer be satisfied as a result of the attack, the more severe the attack is.

Schmitt's description of this criterion has evolved since then, and *Tallinn 2.0* contains its most recent formulation, which includes a way of assessing what falls between the two extremes: "the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force."[33] Now, if states are considered to have accepted the responsibility to be guardians and facilitators of the exercise of human rights under ICCPR, ICESCR, and the other rights treaties to which they are party, then human rights are also a matter of critical national interest because they involve international obligations. Human rights are (broadly and collectively) aimed at human flourishing, and humans cannot flourish if their basic needs cannot be satisfied. This provides a way to assess non-physical harm on the basis of how the attack impinges upon the exercise of human rights: the more fundamental the right that is violated or that the state can no longer support, the more severe the attack is. Widespread death or injury marks the most severe attacks under this interpretation as an arbitrary deprivation of life,[34] while the inability to access bank accounts[35] would not rate highly, and the disruption of the voting process[36] would be somewhere in between. In any case, the target state needs to show how the act violated its sovereignty in order to justify acting in self-defence. If the

[30] *Tallinn 2.0*, Rule 4, comment 16.

[31] *Tallinn 2.0*, Rule 69, comment 9(a).

[32] Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 914.

[33] *Tallinn 2.0*, Rule 69, comment 9(a).

[34] ICCPR, Art. 6(1).

[35] ICESCR, Art. 6(2), understanding access to banking as an economic freedom.

[36] ICCPR, Art. 25(b).

act produces widespread or persistent consequences with respect to those sovereign interests, then the effects are more severe than if they are momentary or localized. On this interpretation, assessing the just-cause criterion of *severity* depends on the significance of what was harmed.

Related to *severity*, but still distinct from it, is the just-cause criterion of *measurability of effects*.[37] All successful cyberattacks have some effects, but not all of those effects are readily apparent or quantifiable. For example, if fifty thousand patients' medical records were at risk of exfiltration due to a piece of spyware, that is a quantifiable risk and a measure of the maximum potential harm. It is not a measure of actual harm. Having a reasonable estimate of the number of records actually exfiltrated gives some idea of the extent of the harm, and is a better guide to the scale of the attack. If the effects of a particular use of force cannot be expressed quantitatively, or if they cannot be discerned at all, then it is difficult to justify claiming that the scale and effects of the action have risen to the level of an armed attack. This is important because in a situation like the logic bomb example, there are no easily measurable effects until the malicious software is triggered. Indeed, the strategic value of compromising an adversary's computing system lies in its remaining undetected until its effects are manifest. While the sports maxim "no harm, no foul" may apply to church-league hockey, it is not clear that it should apply in the context of cyberattacks. The absence of physical harm does not mean the absence of a violation of sovereignty.

This is enough to start classifying cyberattacks as moderate or flagrant. A flagrant cyberattack must be both a violation of state sovereignty (*severity*) with widespread effect (*measurability of effects*). A cyberattack that violates sovereignty but does not have widespread effects is best classified as moderate. A failed cyberattack that produces no effects is not a violation of sovereignty,[38] but can be treated as a moderate cyberattack simply because it posed a threat to a state's sovereignty. Flagrant cyberattacks that clearly satisfy the other cyber just-cause criteria may give reason for a state to consider responding to the cyberattack with a use of force, provided the remaining *jus ad bellum* conditions are also satisfied. That use of force, as argued in Chapter 2, does not have to be made by cyber means, though the proportionality and discrimination obligations of *jus in bello* (Table 2.2) will

[37] *Tallinn 2.0*, Rule 69, comment 9(e).

[38] *Tallinn 2.0*, Rule 4, comment 24.

likely favour a moderate cyber response because it can be precisely targeted without causing the physical collateral damage of a nocuous response. If a moderate response by cyber means is not likely sufficient to end the attack (or threat of another imminent attack), then a kinetic response may be justified as long as it plausibly remains within the bounds of *jus in bello* obligations.

5.3 Applying the distinction

A conceptual framework does not do any good until it is put to use somehow. A few scenarios will demonstrate its value.

Logic bombs and critical infrastructure

Suppose someone discovers a dormant logic bomb on a critical control system, perhaps one at the operation centre for a regional electrical grid. If the malicious code is detected before it is triggered, the cost of removing it and validating the integrity of the affected system is comparable to removing a software virus or recovering from any other incident that accidentally damages data.[39] Any facility of critical national interest should have, for its own sake, operational continuity processes designed to recover from such critical data corruption events.[40] The amount of effort to remove a dormant logic bomb is no greater than what recovering the loss of important data by any other means would be. Since typical hardware failures or software crashes are not armed attacks, and since the harm of a dormant logic bomb, once discovered, is comparable to the harm done by such a failure, it is not reason-

[39] Executable code is merely data processed by the more basic programs encoded in the circuitry of a computer's instruction-processing unit. System failures that affect data storage and transmission can affect executable code, since that code is stored and transmitted using those data systems.

[40] Some states and organisations have mandated this. Two examples are documented in United States President, *Critical Infrastructure Protection*, Presidential Decision Directive/NSC 63 (May 22, 1998), accessed August 15, 2016, `https://fas.org/irp/offdocs/pdd/pdd-63.pdf` and Commission of the European Communities, *Communication from the Commission on a European Program for Critical Infrastructure Protection*, COM(2006) 786 (Brussels, BE, December 12, 2006), accessed August 15, 2016, `http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN`.

able to consider the physical harm to a state caused by the mere placement of a logic bomb as anything more than an operational inconvenience.

In this example, the logic bomb would score highly on the severity criterion because it targeted the electrical grid—a critical national interest for supporting the economic and social functions of government. It would not be a direct infringement of fundamental human rights. Even though persons whose jobs rely on electricity being readily available would not be able to work temporarily, their right to work would not impaired. The most significant rights targeted by the logic bomb are the loss of access to health care[41] and the "benefits of scientific progress"[42] that facilitated the development of the electrical grid. Because there is no physical damage and no lasting—if any—effect on critical national interests, there is no discernible or significant harm to compare against the scale and effects of an armed attack. Such a cyberattack would be classified as a moderate one and not a flagrant one simply because the effect is minimal with respect to physical harm. This does not mean it is without cost to repair, but that kind of cost is not one that factors into the *jus ad bellum* deliberation. Thus there is no basis for a state to claim that another state's placement of a logic bomb is an armed attack unless and until the malicious code is actually triggered.

However, placing such a logic bomb is, at least in terms of invasiveness and potential harm (regardless of intent to produce it) is still something that could look like a use of force against the target state. This meatspace analogy, based on the Halifax harbour explosion on December 6, 1917, reveals the disanalogy between aggressive but non-damaging actions by cyber and conventional means.[43] Suppose that the munitions-laden freighter *Mont Blanc*, instead of being struck by the *Imo*, had been the target of an assault from a handful of German Friedrichshafen G.III bomber aircraft that somehow made the trip across the Atlantic Ocean.[44] If the bombers had succeeded in hitting the *Mont Blanc*, the bombing could be treated as a permissible armed attack within the current laws of armed conflict: a formal state of war existed between Canada and Germany; the harbour was a target with

[41] ICESCR, Art. 12(d).

[42] ICESCR, Art. 15(b).

[43] I thank Mathieu Doucet for this example.

[44] Dan Alex, "Friedrichshafen G.III Bomber/Night Bomber Aircraft," *Military Factory*, July 31, 2019, accessed September 17, 2020, https://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=602.

military value; and the resulting damage to the civilian portions of the city, despite being disproportionate to what would have been required to neutralize the harbour, could still be deemed as acceptable collateral damage provided the aircrews had no knowledge of the *Mont Blanc*'s cargo. Even if the bombers had missed the *Mont Blanc* or any of the other ships in the harbour area and the bombs had all failed to detonate, sinking harmlessly in the water, the bombing run itself, without causing physical harm, would be a use of force because of its invasive nature. Further, the threat of physical damage, including civilian deaths, would be apparent as soon as the aircraft were detected. A proportionate defensive move would be to shoot the aircraft down—a justifiable, nocuous response even though no harm was inflicted.

The failed or defused logic bomb is just as invasive as the bombing run, but the intended outcome and the extent of the potential physical harm are not nearly so clear as they are in a failed bombing run. In the case of a thwarted logic bomb where there is no knowledge about intended and potential outcomes, it seems that the proportionate defensive response to the cyberoperation must be something less forceful than a nocuous counterstrike.[45] Even a moderate counterstrike may not be permitted, since removing the malware ends the threat without the need for a counterstrike. So while a use of force by cyber means is not significantly different from a conventional use of force with respect to invasiveness or violation of sovereignty, the state of knowledge with respect to any threatened or intended physical harm constrains the target state's response. The significant difference between the failed logic bomb and the failed harbour bombing is epistemic, not metaphysical. If the logic bomb had been activated, and it succeeded in producing an uncontrolled shutdown of the electrical grid, leading to equipment-destroying overloads in generators, transformers, and interconnections, that is enough physical harm to be considered an armed attack since even a precision bombing run would produce the same effect. The cyberattack would then legitimately be called flagrant. This still does not mean a use of force is permitted in response, but it satisfies the severity and measurability of effects criteria for determining just cause.

The cascading failure of part of the eastern electrical interconnection during the blackout of August 14, 2003, illustrates the economic disruption that

[45] *Tallinn 2.0*, Rule 22, comment 10; Rule 69, comment 11.

could result from a cyberattack on the electrical grid. This outage affected portions of Ontario, Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey.[46] Some areas were without electricity for four days, while areas had reduced supply managed for a few days by rolling blackouts or keeping large industrial consumers shut down.[47] This outage went beyond a mere inconvenience to being a significant economic disruption for business, industry, transportation, and individuals. "Estimates of total costs in the United States range between $4 billion and $10 billion (US dollars). In Canada, gross domestic product was down 0.7% in August, there was a net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down $2.3 billion (Canadian dollars)."[48] Yet there was no penalty imposed on the company for the economic damage because American law at the time "[did] not require electric reliability standards."[49]

The international report on the causes of the 2003 blackout explicitly ruled out a cyberattack as a contributing factor to that incident.[50] However, it did note that "[m]any malicious code attacks, by their very nature, are unbiased."[51] In other words, they do not necessarily seek out particular targets, just systems that happen to be vulnerable to the attack. It turns out that the company responsible for the August 2003 blackout had been the victim of an indiscriminate piece of malware a few months before. The incident took place at an off-line nuclear plant when "the 'Slammer' Internet worm took down monitoring computers. . . . A subsequent report . . . concluded that although the infection caused no outages, it blocked commands that operated other power utilities."[52] DDOS attacks may also be indiscriminate,

[46] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, causal analysis (April 2004), 1, accessed September 29, 2020, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[47] U.S.-Canada Power System Outage Task Force, 1.

[48] U.S.-Canada Power System Outage Task Force, 1.

[49] Reuters, "DOE Chief Sees No Blackout Penalty for FirstEnergy," November 19, 2003, accessed September 29, 2020, https://web.archive.org/web/20040224080845/http://www.forbes.com/markets/newswire/2003/11/19/rtr1153863.html.

[50] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, 132.

[51] U.S.-Canada Power System Outage Task Force, 133.

[52] U.S.-Canada Power System Outage Task Force, 132.

where the target system is whatever happens to be at the end of the network address generated pseudorandomly.[53] Another part of the epistemological problem around responding to an aggressive cyberoperation, then, is discerning whether the attack is specifically aimed against the affected system, a nuisance assault against a target of opportunity, or just rogue software autonomously discovering and exploiting a system vulnerability.

Elections and other social functions

There is growing recognition that physical harm is not the only kind of harm that can jeopardize the sovereignty or integrity of a state. The logic bomb scenario shows how physical harm producing economic and institutional disruption can follow both conventional and cyber attacks. Conventional attacks will do this by physical means, so there is clear evidence of an armed attack having taken place. In the cyber context, however, there may be no intermediate physical harm apparent. There is no need for a cyberattack to cause physical harm to disrupt economic or institutional functions. Moreover, a cyberattack does not even need to install malicious software on the target system to cause these kinds of harm. All it has to do is overwhelm the target system's ability to communicate with other systems. As the 2007 cyberattack against Estonia (discussed in Chapter 3) demonstrated, a well-coordinated long-duration DDOS attack can bring a halt to electronic transaction processing, including the trading of securities, commodities, and derivative instruments. This would bring electronic commerce to an effective halt, impairing the sale of goods, the fulfillment of contracts, and the flow of money. If the target is a distributed database or equipment that facilitates fair elections, the disruption could undermine the legitimacy of the election.

The *Tallinn Manual* acknowledges that cyberoperations causing effects that do not rise to the level of an armed attack or even to the level of a use of force may still violate international law.[54] If a state's government or armed forces participates in or enables this kind of disruptive cyberattack without causing physical harm, it still seems reasonable to treat it as violation of a state's sovereignty over its affairs. In other words, it is at least a moderate

[53] Pseudorandom numbers are generated algorithmically and are not truly random. They are "random enough" for most purposes, such as producing a number between 0 and 255. Four or eight such numbers make up an Internet address.

[54] *Tallinn 2.0*, Rule 68, comment 6.

cyberattack, though not likely a flagrant one. For example, if an election is disrupted by another state, that state has usurped one of the "inherently governmental functions" of a state,[55] something that is recognized as a violation of sovereignty. It also violates the right of citizens to participate in elections in a way that "guarantee[s] the free expression of the will of the electors."[56] Ending the threat may mean discarding the election results. It is not clear, though, that there are any effective countermeasures the state can take while the threat of disruption is still active without halting the voting process itself.[57] Disrupting an electoral campaign through disinformation attacks and faking grass-roots support for a particular position (a technique called *astroturfing*) through social media is a social engineering attack done through cyber means, but because it does not result in physical harm, it is not a flagrant cyberattack.[58] It is not even a violation of sovereignty, but a presumptively legal means of communication "designed to achieve national objectives."[59] These kinds of state-involved cyberoperations can be considered no more than moderate cyberattacks because they are not clear violations of sovereignty.

Economic disruption

The disruption of an economy by cyber means is a complex case. There is currently neither widespread state practice nor international law on this

[55] *Tallinn 2.0*, Rule 4, comment 10.

[56] ICCPR, Rule 25(b).

[57] Computer scientists and software designers are almost unanimous in the opinion that elections should not take place over the Internet. The Internet fundamentally operates on the trust of its users, and any security methods are sophisticated afterthoughts. Voters will not reliably take measures to secure their ballots. The secrecy of the ballot cannot be guaranteed, and digital credentials are readily forged, so a person intending to vote may discover that the ballot intended for them has already been marked as being cast. Digital ballots are easily intercepted and altered, and the altered ballots can be recorded in the audit trail. Governments, however, have a habit of not listening to experts. A network completely separated from the Internet could be secured, but at a greater cost than using paper ballots and tallying them by scanners or by hand.

[58] *Tallinn 2.0*, Rule 69, comment 3.

[59] Department of Defense [USA], *Joint Publication 3-13.2: Psychological Operations* (January 7, 2010), 1.2.a, b, accessed February 5, 2021, `https://fas.org/irp/doddir/dod/jp3-13-2.pdf`.

point.[60] However, "[e]conomic coercion is presumptively lawful"[61] under the international law of sanctions—which are still intrusions upon the sanctioned state's sovereignty but explicitly declared not to be a use of armed force against it[62]—developed during the creation of the UN Charter.[63] Economic sanctions have been considered the least disruptive way of exercising pressure on a state to change its behaviour without resorting to armed intervention, and were designed to bar the sanctioned state's claim to self-defence. It turns out that in many cases the effects of these sanctions affect the well-being, and perhaps threaten the lives, of the state's civilian population (a violation of the inherent right to life[64] if death does result, or perhaps of the right to freedom from "cruel, inhuman or degrading treatment or punishment"[65] if it does not). Neither of these outcomes seem to be in line with sanctions' intended purpose, and both of them, outside of sanctions, give a state some support for a claim of self-defence to protect the rights of its civilians.[66] A further complication is that in the context of armed conflict, sanctions look a lot like a collective penalty against civilians for offences they did not commit, which is prohibited under Article 33 of GC IV. It is inconsistent, perhaps even absurd, for a freedom to be asserted under the laws of armed conflict when it is not one recognized during times of peace. If a state of peace between nations is asserted as the desired and normal state of affairs (which the preamble to the UN Charter affirms), and if particular rights are given protection under the laws of armed conflict (which the Geneva Conventions affirm), then those rights must exist during peacetime so that the laws of armed conflict have something to protect. (In other words, war is not the kind of action that can establish fundamental human rights, but the almost routine claims of human rights violations during war demonstrate the existence of fundamental human rights both prior to and

[60] *Tallinn 2.0*, Rule 4, comment 28.

[61] *Tallinn 2.0*, Rule 69, comment 10.

[62] UN Charter, Art. 41.

[63] *Tallinn 2.0*, Rule 69, comment 2

[64] ICCPR, Art. 6.

[65] ICCPR, Art. 7.

[66] Public statements do not necessarily reflect geopolitical reality. Nonetheless, a state can assert the claim without requiring international verification of the reasoning before taking action in self-defence. However, if such action is taken, *ex post facto* disproof of the claim will not undo the consequences. Consequently reparations, further sanctions, or armed humanitarian intervention may be in order.

during the conflict. This makes *post bellum* recovery of the ability to exercise rights an important means of avoiding a future war.) Therefore, as a violation of rights in peacetime, and what would be a violation of the laws of armed conflict during wartime, economic sanctions look like they would provide just cause for a use of force in response were it not for the exception carved out for them under international law.

Sanctions are not the only means of economic coercion or disruption. Though a state's economy is a critical national interest, the health and stability of a state's economy is connected to the health and stability of the economies of its largest trading partners. It is presumptively legal to use trade mechanisms to interfere with a state's economy in pursuit of political goals (for example, Canada's application of retaliatory tariffs in 2018 against a narrow selection of American goods that just happened to be produced in Trump-supporting regions[67]).

Using cyber or kinetic means to disrupt an economy is a different matter. In general, national economies are not solely connected to legitimate military targets. Though some parts of the economy directly support military activity, the parts that do not cannot be targeted without violating the principle of discrimination.[68] A state-involved cyberattack intended solely to produce an economic advantage against the target state, and not to coerce a change in the target state's policies, will be most effective if it targets a critical, non-military national interest such as its financial markets. Such a cyberattack is a clear violation of sovereignty and of the laws of armed conflict.[69] The measurable effects of the cyberattack would determine whether it is a moderate cyberattack that can be considered a use of force or a flagrant one equivalent to an armed attack. In either case, a cyberattack against a state's economic interests may provide just cause for a use of force in response, provided the other just-cause criteria and *jus ad bellum* conditions are satisfied.

[67]W. Jim Jordan et al., *With a Clear Conscience: Business Ethics, Decision-Making, and Strategic Thinking*, ed. Gregory G. Andres (Don Mills, ON: Oxford University Press, 2021), 214.

[68]*Tallinn 2.0*, Rule 100, comment 21.

[69]Owens report, 259.

5.4 Responsibilities for mitigation

While target states have to justify responding to an aggressive cyberoperation by making reference to scale and effects (along with the other just-cause criteria and *jus ad bellum* conditions), an attacking state may make the rhetorical claim that its target state has some responsibility to mitigate the harm arising from an attack so and must bear some of the blame for the extent of the harm if it had not taken steps to mitigate that harm. However, taking advantage of a state's unpreparedness or inability to mitigate the harm does not change the fact that a harm has occurred. Claiming that the target state had responsibility to mitigate an attack merely and unjustly attempts to shift the blame, for mitigation would not have been necessary if the attack had not been made. So international law permits a target state to take countermeasures in self-defence before beginning any possible mitigation activity.[70] In other words, stopping the harm is acknowledged to have higher priority than allowing harm to continue until no further mitigation is possible.

Even so, a state does have responsibility for defending its civilians "to the maximum extent feasible . . . against the dangers resulting from military operations"[71] during times of armed conflict. With respect to cyberwar, not only is it in a state's military interest to secure the computing and communication networks that support critical military infrastructure against aggressive cyberoperations, but it is also in the state's interest to do the same for critical civilian infrastructure.[72] All this entails is securing enough of the network infrastructure, on a best-effort basis, to protect any life- and rights-sustaining functions that must be conducted over a computer network.[73] There are existing international technical standards that describe ways to do this from a perspective that incorporates hardware and software reliability, secure network communication protocols, and organizational compe-

[70] *Tallinn 2.0*, Rule 23, comment 9. This also means that the countermeasures can be proportionate to what is needed to end the harm being done without taking into account any mitigation the target state might be able to do concurrently. The failure to mitigate may affect the calculation of reparations if it can be shown that the target state intentionally delayed it to inflate a claim for reparations, but it does not affect the permissible forcefulness of the response. *Tallinn 2.0*, Rule 28, comment 8.

[71] AP I, Art. 58.

[72] *Commentary on the Additional Protocols*, ¶2240; *Tallinn 2.0*, Rule 121.

[73] *Tallinn 2.0*, Rule 121, comments 9, 12.

tencies and responsibilities.[74] If a state is home to businesses that find it important to invest in cybersecurity to protect themselves from data theft, malware, and operational failure as a legal defence from criminal and civil judgements when the almost-inevitable breach does occur, then it is at least equally important for the state's military organizations to do so where the stakes (state sovereignty, human lives, environment) are higher.

States originally uninvolved in a conflict may become unwilling agents in it when cyberattacks are routed through network infrastructure in their territory. These third-party states have the international responsibility "not to allow knowingly its territory to be used for acts contrary to the rights of other states."[75] While this principle of "due diligence"[76] was first applied in

[74]International Organization for Standardization and International Electrotechnical Commission, *International Standard ISO/IEC 27000: Information Technology—Security Techniques—Information Security Management Systems*, technical standard, ISO/IEC 27000:2018(E) (Geneva, CH: International Organization for Standardization, February 2018), https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip (hereafter cited as ISO/IEC 27000) provides guidance for organizations and government departments concerning information and network security in general. ASTM International, *Standard Guide for Cybersecurity and Cyberattack Mitigation*, technical standard, F3286-17 (West Conshohocken, PA: ASTM International, December 1, 2017), accessed September 1, 2020, https://doi.org/10.1520/F3286-17 (hereafter cited as ASTM F3286) specifically addresses mitigating the effects of cyberattacks, while ASTM International, *Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)*, technical standard, F3201-16 (West Conshohocken, PA: ASTM International, September 1, 2016), accessed September 1, 2020, https://doi.org/10.1520/F3201-16 (hereafter cited as ASTM F3201) and ASTM International, *Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems in Accordance with IMO Resolution MSC.428(98)—Cyber Risks and Challenges*, technical standard, F3449-20 (West Conshohocken, PA: ASTM International, June 1, 2020), accessed September 1, 2020, https://doi.org/10.1520/F3449-20 (hereafter cited as ASTM F3449) establish practices for system security and risk management in uncrewed aircraft and maritime vessels, respectively. A longer list of relevant ISO/IEC security standards is provided in O.M. Fal', "Standardization in Information Technology Security," *Cybernetics and Systems Analysis* 53, no. 1 (January 2017): 78–82, https://doi.org/10.1007/s10559-017-9908-8.

[75]International Court of Justice (ICJ), *Corfu Channel case*, 1949 ICJ 4, April 9, 1949, 22, accessed April 25, 2016, http://www.icj-cij.org/docket/files/1/1645.pdf (hereafter cited as *Corfu Channel*), referenced in *Tallinn 2.0*, Rule 6, comment 2. The judgement also states here that this is not an obligation imposed by a signed international convention; rather, this obligation predates the 1907 Hague Conventions as one of the "certain general and well-recognized principles" alluded to in those conventions.

[76]*Tallinn 2.0*, Rule 6, comment 1.

a maritime context,[77] this principle can also apply in a cyber context due to the fundamental design of the Internet and its protocols.

Internet transmissions consist of small *packets* of data. Each packet can take a different route to its destination. Because the Internet is global in scope, Internet traffic routinely crosses international boundaries.[78] Some of this traffic is malicious or exploitive in some way.[79] Cisco Systems reported that 11.6% of the identifiably malicious traffic passing through its brand of network equipment in 2015 was aimed at infiltrating, disrupting, or disabling small-scale industrial control systems (ICS) and larger-scale supervisory, control, and data acquisition (SCADA) systems.[80] Internet-connected

[77] On October 22, 1946, two British warships claiming innocent passage through the Corfu Channel (which includes some Albanian territorial waters) struck moored mines in an area that had been clear of mines less than six months earlier. Many officers and crew were injured, and some were killed. Even though Albania likely did not lay the mines, it was established that Albania knew about them, and failed to warn the British ships of the danger.

[78] For example, any Internet traffic between a computer at my home in Kitchener and my hosting service in Toronto is usually routed through Chicago, because that is where my Internet service provider makes its most efficient connection to my host's Internet service providers.

[79] There is no consensus estimate of what proportion of Internet traffic serves malicious purposes, but there are some measures of it for major Internet-based applications. World-Wide Web traffic is only a portion of Internet traffic, and roughly 30% of that portion is malicious. Imperva, Inc., "Incapsula Finds Malicious Bots Account for Approximately 30 Percent of Internet Traffic," Imperva, Inc., December 29, 2014, accessed April 28, 2016, https://www.incapsula.com/about/press-releases/incapsula-finds-malicious-bots-account-for-approximately-30-percent-of-internet-traffic/. Similarly, of the roughly 347 billion email messages per day that passed through one vendor's equipment, about 85% of it was *spam*, and another 76 million messages per day contained malicious software (*malware*). Cisco Systems, *2015 Annual Security Report*, technical report (San Jose, CA: Cisco Systems, 2015), accessed April 28, 2016, http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf. More than 50% of all Internet traffic is now encrypted, and it is not possible to inspect encrypted data packets to see if a message contains malware. Cisco Systems, *2018 Annual Security Report*, technical report (San Jose, CA: Cisco Systems, 2018), 9, accessed March 2, 2021, https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf. Nonetheless, some malicious software does use encryption to obfuscate its purpose. Sandvine Incorporated ULC, *2016 Global Internet Phenomena: Spotlight: Encrypted Internet Traffic*, technical report (Waterloo, ON: Sandvine Incorporated ULC, February 2016), accessed April 28, 2016, https://www.sandvine.com/downloads/general/global-internet-phenomena/2016/global-internet-phenomena-spotlight-encrypted-internet-traffic.pdf.

[80] Cisco Systems, *2015 Annual Security Report*, 9. Cisco has not published comparable data

command-and-control (C2) systems are prized targets for certain kinds of malicious software, and military C2 systems may be legitimate targets for a state-led network-based attack.

Even though the attacking state and target state may share a geographic border, there is no guarantee that any network traffic between the two states will not traverse other states' networks. The data packets associated with that activity may well travel through third-party states' Internet infrastructure simply because of the way Internet routing works. This happens automatically; the intermediate states receive no notification from the Internet itself that an attack is using their network infrastructure,[81] and the attacking state has no way to force a particular routing.[82] It is possible, and highly probable, that third-party states will not be aware of the cyberattack being conducted over their Internet infrastructure. Once an intermediate state is aware of the operation taking place over its Internet infrastructure, satisfying the "due diligence" requirement concerning harm to another state gives rise to another obligation: that intermediate state is expected to do what is feasible to end the internationally unlawful use of their cyber infrastructure.[83] It may be that the intermediate state will learn of the cyberattack

---

since this report.

[81] *Tallinn 2.0*, Rule 6, comment 14.

[82] Unlike the wired telephone network, the Internet does not rely on a single continuous physical connection between two terminals. Each router (a device that forwards Internet packets to either their destination or to another device between it and each packet's destination) in a service provider's network usually has connections to multiple other routers (some of them owned by other service providers), and the owners of each router will program a preferred forward route to other parts of the Internet on the basis of cost, availability, or some other metric. If the preferred route is not available, the next-best one will be chosen, and so on. Because most Internet transmissions need multiple data packets to hold the full content of the transmission, each packet can follow a different route from its source to the destination, and those packets can arrive in a different order than they were sent. The system on the receiving end will reassemble the message when all of the packets have been received. The only way to force an Internet transmission to a single route is to have control over *all* of the physical routes between the origin and the target, and program only a single route from source to destination. This principle also facilitates national firewalls. For example, all Internet traffic to and from China goes through a small number of state-controlled routers. Packets going to or arriving from banned services can be intercepted and discarded at those border gateways, but state-approved traffic will be forwarded on.

[83] *Tallinn 2.0*, Rule 7. However, determining when this is happening is not easy to do in a timely fashion, and any encryption involved makes it even harder.

only after the target state begins taking countermeasures against it. These countermeasures against a third-party state are permissible as long as they are proportionate to what is required to end the harm, and they must cease when the third-party state begins taking its own action to end the harm.[84]

Having this responsibility as a third-party state and having the means to fulfil it are two different things. Among the ugly realities of cyberwar is an asymmetry in cost. Cyber offence can be very cheap and in crude cases does not require a high ratio of hits to attempts for the attack to be effective. Conversely, cyber defence can be prohibitively expensive while still being ineffective.[85] This is why the means taken do not go beyond what is feasible (understood as "reasonably available and practicable"[86]) for the third-party state to do, either on its own or with contracted assistance.[87] However, if a state does have the means to fulfil this obligation, then it also has some ability to secure and defend its own cyber infrastructure, and this is where network defence brings the obligations to its civilians and to other states together. If a state has some ability to mitigate the impact of malicious network traffic directed its way, then it has some of what it needs to defend its civilian population from any death or injury that might otherwise arise from such activity.

This gives rise to another cyber just-cause wrinkle. If a state is not defending its civilian population from another state's attacks, or if a state is violating its citizens' rights, it may be subject to international intervention under emerging "responsibility to protect" reasoning. As Edward Barrett suggests, "[s]tate actors who abuse their citizens lose their authority, their citizens have a right to rebel and waive their right to non-interference, and other states capable of providing security have obligations to do so."[88] While this reasoning is often proposed with respect to conventional means of war (air strikes against government forces, followed by troops and humanitarian relief on the ground), it seems that it could also apply when cyber means are involved. One way is to intervene using cyber means to thwart ongoing

[84] *Tallinn 2.0*, Rule 21.

[85] Owens report, 13.

[86] *Tallinn 2.0*, Rule 7, comment 2.

[87] *Tallinn 2.0*, Rule 7, comments 16, 17, 19.

[88] Edward T. Barrett, "Warfare in a New Domain: The Ethics of Military Cyber-Operations," *Journal of Military Ethics* 12, no. 1 (April 2013): 9, https://doi.org/10.1080/15027570.2013.782633.

rights violations (though admittedly most rights violations leading to third-party intervention would likely be those associated with the necessities of life and so need a meatspace intervention alongside any cyberspace one). The other way comes when cyber means are used to violate those rights, such as "losing" civil records, denying access to services that are only provided online, or violating privacy by searching personal data for the purposes of suppression or harassment. Both of these could provide just cause for a use of force (kinetic or cyber, depending on proportionality and discrimination obligations) against the offending state, provided other *jus ad bellum* conditions are met. Whatever the means, they must not add to the harm already being done to the civilian population.

This second way has caught the attention of another international organization: the International Monetary Fund (IMF). The IMF has adapted this idea, proposing a way for external states to advance and protect rights using non-forceful means during peacetime. In its quest to bring digital financial services to the "1.7 billion [adults worldwide who] are still unbanked,"[89] the IMF has issued a call to "[help] developing and emerging economies build cybersecurity capacity."[90] This is one possible way for smaller and poorer states to secure their national infrastructure to some minimal standard that provides at least some protection to citizens' financial data and safeguard the right of citizens to some degree of economic freedom.[91] This call, as self-serving as it may be to the wealthy states in the global financial community, is nominally in accordance with the states parties' covenant "to take steps . . . through international assistance and co-operation, especially economic and technical, . . . with a view to achieving progressively the full realization of the rights recognized" in the ICESCR.[92]

On one reading of this paragraph in the treaty, it may be considered a violation of an international obligation for a state party to ICESCR to refuse to

[89]Kristalina Georgieva, "Financial Inclusion and Cybersecurity in the Digital Age," International Monetary Fund (IMF), speech delivered to (Virtual) Conference on Financial Inclusion and Cybersecurity, December 10, 2020, accessed February 19, 2021, https://www.imf.org/en/News/Articles/2020/12/10/sp121020-financial-inclusion-and-cybersecurity-in-the-digital-age.

[90]Jennifer Elliott and Nigel Jenkinson, "Cyber Risk is the New Threat to Financial Security," *IMFBlog*, December 7, 2020, accessed February 19, 2020, https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/.

[91]ICESCR, Art. 6(2).

[92]ICESCR, Art. 2(1).

provide another state party the necessary means to develop cybersecurity to the level where the state can participate in the international banking system. But this level of cybersecurity will also help a state secure its military and remaining publicly-owned civilian infrastructure. Further, it is a level of security that may prevent or blunt some of the harm caused by a cyberattack, satisfying the best-effort obligation to defend citizens from those harms. It may also keep the state from being an unknowing third-party conduit for a cyberattack against the financial systems of another state (which might provide motivation for external states to provide this assistance). In theory, at least, states without the means to secure their cyber infrastructure can ask for help, and states that can help must do so on a best-effort basis. Still, a state is not under any obligation to request this assistance, and not requesting or refusing an offer of this assistance does not diminish an aggressor state's responsibility for harm done by a cyberattack.

5.5 Separating the causal and the temporal

In the same way that a neutral state's duty to not allow its cyber infrastructure to be used by an aggressor to harm other states depends on knowing that an aggressive cyberoperation is in progress, a state's duty to protect its civilians from certain cyberattacks also depends on having that knowledge. This brings in a temporal consideration for determining whether just cause for a forceful response exists. The time at which a state becomes aware of a cyberattack may affect whether the cyberattack is moderate or flagrant. In situations where there is sufficient knowledge to determine the origin, intention, and potential harm of an attack, the scale-and-effects doctrine provides consistent guidance in assessing the just-cause criteria of severity and measurability of effects. When the temporal and causal distances from the initial action to the resultant and anticipated harm are added to the mix, the guidance becomes more conflicted. I will present examples where a state has committed an act that violates the target state's sovereignty that, by itself, would not be a flagrant attack, but the direct consequences, when they become apparent days or months later, would. In light of the scale and effects resulting from the initial act, regardless of how far separated they are temporally, knowledge of the effects at the time of the initial action might contribute toward having just cause for a forceful response, yet any ability

for the target state to mitigate any unrealized effects limit the character of any response. I have argued that it is difficult to justify an armed response when the effects are minimal; now I will further argue that it is also difficult to treat a state's capability to cause harm as sufficient just cause for a forceful response when there is no indication that the state intends to inflict that harm. Moreover, I will show by analogy that the concerns about cyberwarfare in this regard are current problems with conventional means of warfare.

It is easy to conflate the causal and temporal distances between an action and its ultimate effect. A typical armed attack has a visible cause (say, a missile launch or armoured vehicles crossing a border) that produces a visible effect (an explosion or the seizing of territory) a short time later. But the relationship between the number of links in the causal chain and the length of the timeline is not necessarily proportional. For example, the *Tallinn Manual*, in its discussion on perfidy, specifically cautions that "[p]roximate cause should not be confused with temporal proximity,"[93] because the actions and communications that invite an adversary's (limited) trust can occur some time before the treacherous strike against that adversary occurs. A cyberattack can follow a similar pattern. A state can begin cyberoperations that leave its adversary unknowingly at risk of harm, and then wait patiently for an opportune time to make the damaging strike.

This caution is relevant to acts of aggression that do not involve perfidy. Suppose an enemy saboteur, operating under military direction and wearing military insignia (making it explicit that this example includes military involvement), has managed to infiltrate a hydroelectric generating station and loosen a few bolts on a turbine housing. This allows the housing to vibrate just a little more than safe operation permits. If this excess vibration continues for a long enough time, the other bolts will bear more stress and the resulting strain will eventually cause them to fail. The now-free turbine will launch upward and a jet of water will follow it. Depending on other circumstances, this could lead to a series of explosions due to pressure, temperature shock, electrical arcing, or a chemical reaction. If these take place near enough to the dam, they could weaken the dam, which may, in turn, collapse.[94] While the root cause of the failure is the saboteur loosening the

[93] *Tallinn 2.0*, Rule 122, comment 6.

[94] An accident at the Sayano-Shushenkaya hydroelectric generating station in Siberia in

bolts, and it can even be considered a proximate cause, this could have been done weeks before the mechanical failure occurred. In this particular case, then, there is a short causal chain between the sabotage of the turbine and the collapse of the dam, but there is an extended period of time between the two events.

Now consider a logic bomb similar to Stuxnet that, when triggered, varies the spin rates in a turbine while intercepting and replacing equipment-generated status reports with ones that indicate everything is operating normally. The varying spin induces a wobble. The wobble slowly loosens the bolts. The bolts eventually shear off, giving rise to the same catastrophic effects as the sabotage case—perhaps even up to the failure of the dam itself. One proximate cause is the placement of the malicious code. Another proximate cause would be the triggering event, but that would not have been part of the causal chain had the logic bomb not been in place to respond to the event. This causal chain, in terms of macro-scale events, is no longer than in the case of physical sabotage: the placement of the logic bomb is equivalent to the infiltration, and the usurping of the control software is equivalent to inducing the vibration that starts the process of loosening the bolts. Everything else follows in the same way.[95] As in the sabotage example, there may be a long period of time—perhaps months—between the placement of the code and that code being triggered, followed by the additional time needed for the physical system to fail as intended.[96] Just as in the sabotage case, the aggressive cyberoperation's destructive effects do not follow immediately (with respect to time) after the placement of the code, though they are closely causally connected to that placement.

2009 produced all but the dam failure. The official root causes were inadequate maintenance and safety controls. Fabian Acker, "Fatal Failures: Siberia's Hydro Disaster," *Engineering and Technology Magazine* 6, no. 7 (July 11, 2011), accessed March 28, 2016, `http://eandt.theiet.org/magazine/2011/07/siberia-hydro-disaster.cfm`.

[95]What counts as a macro-scale event is somewhat subjective. Faking controller reports might be seen as a separate event, but it is another chain that follows from the triggering of the logic bomb that runs parallel to the effects produced in the turbines, and not part of the same chain.

[96]The intended effect may have been only to stop the generation of electricity for a military facility. The dam failure may not have been intended. However, if the dam had failed, the attacking state would be responsible for the downstream effects, as the failure of the dam is out of proportion to the military advantage sought by ending electricity production. *Tallinn 2.0*, Rule 113, comment 8.

These examples show that causal proximity and temporal immediacy, while they often run together, can come apart in one direction: a short causal chain with a long period of time between the initial aggressive act and the manifestation of its intended effects. But they can come apart in the other direction, too. A conventional aerial bombing has a longer chain of discrete events: making weather observations and forecasts; briefing the crew; assembling, loading, and arming ordnance; installing cameras to capture images for assessing the effectiveness of the attack; performing aircraft readiness checks; outfitting the aircrew; coordinating an ordered launch of multiple aircraft; gathering aircraft from several bases in groups at an in-flight assembly point; dividing into attack squadrons; dodging anti-aircraft fire; dropping the bombs; and—if all has gone well with respect to the mission—returning to base.[97] All of this takes place in the span of about twelve hours. Launching the aircraft indicates at least readiness to attack, and is a use of force, but until the aircraft enter the target state's airspace and drop their payload, an armed attack has not taken place.[98] The use of force to that point has not produced a significant harm to the victim state, and the anti-aircraft fire is the proportionate response to reduce the threat. This scenario has a comparatively long causal chain compared to deploying a logic bomb, which has no need for crew briefing and outfitting, ordnance preparation, pre-flight checks, marshalling, or a safe return to base. The air strike has a short period of time between the beginning of the armed attack (not the use of force, which began at takeoff) and the first of its effects.[99] So the temporal and causal chains of any harm can vary in length independently of the

[97]Annette Tison, "Anatomy Of a Bombing Mission," *392nd Bomb Group*, 2017, accessed October 1, 2020, `https://www.b24.net/MissionAnatomy.htm`.

[98]The imminence of an armed attack may justify a preemptive use of force in "anticipatory self-defence," but that is another study. *Tallinn 2.0*, Rule 73, comment 2, with reference to Derek William Bowett, *Self-Defence in International Law* (New York, NY: Frederick A. Praeger, 1958), 188–89. Any use of force in response must be proportionate to what is required to end the threat of an imminent attack.

[99]Geology provides another analogy. An earthquake is caused by a slow build-up of strain along a fault line. The strain along parts of the fault may be relieved by sporadic smallish earthquakes (foreshocks). However, when a segment under a great deal of strain (with respect to geological processes) ruptures, the time it takes to release that stored energy along its length results in prolonged shaking that induces the catastrophic effects. The longer the intense shaking persists (*ceteris paribus*), the more damage there is. The point is a long causal chain of discrete events can produce catastrophic effects in a comparatively brief period of time. Luc Reychler, *Time for Peace: The Essential Role of Time in Conflict and Peace*

other. This means that the evaluation of any act of aggression, be it cyber or conventional, must assess the just-cause criteria of temporal *immediacy* and causal *directness* separately.

5.6 Aggressive cyberoperations and distant effects

The logic bomb and airstrike examples show that effects reaching the level of an armed attack can result from both a use of force that had been initiated at some comparatively distant time in the past and had lain dormant until triggered, and also from more causally complex uses of force that run to completion over a short period of time. However, both extended causal chains and extended periods of time provide some opportunity to mitigate—or even eliminate—the harm that the aggressive action had the potential to produce. The temporal framework from the Owens report[100] diagrammed in Figure 5.1 is a good starting point for analyzing whether a cyberattack meets the just-cause criteria of *immediacy* and *directness* that would make it a flagrant cyberattack.

In the example of the logic bomb in the hydroelectric generator control system, the causal chain between its placement and producing the intended harm is quite short. Unlike the Rube Goldberg-style device contructed in the table game *Mouse Trap*,[101] there are few discrete macro-level events between $T_{compromise}$, the time the logic bomb is successfully deployed, and $T_{effects\ apparent}$, the time when the first turbine fails. The events just take a long time to develop. There is no question that its placement is a violation of sovereignty if it can be traced to a state (or an agent acting on behalf of a state) that seeks a military gain of some sort.[102] If the malicious code

Processes (Brisbane, AU: University of Queensland Press, 2015).

[100] Owens report, 89–90.

[101] *Mouse Trap* was first published in 1963 by Ideal Games. The goal is to avoid having your mouse-shaped game token captured by the trap. Todd Coopee, "Mouse Trap by Ideal (1963)," *Toy Tales*, June 29, 2018, accessed May 7, 2020, `https://toytales.ca/mouse-trap-ideal-1963`. Operating the trap meant initiating a chain of 13 discrete triggering actions in a process that has additional points of potential failure between the triggers. The whole process, if it worked, would take about 20 seconds. Terry Beck, "Mouse Trap Game in Slow Motion 19 Seconds," video recording, April 27, 2015, accessed May 7, 2020, `https://www.youtube.com/watch?v=sy840XvnQRA`.

[102] *Tallinn 2.0*, Rule 69, comment 9(f), (g).

runs to completion and causes damage that includes loss of life or harm to property, then the effects make the whole extended episode a flagrant cyberattack equivalent in effects to an armed attack, and it would be reasonable to say that the armed phase of the attack began at $T_{compromise}$ (Figure 5.1(b), (e)).

However, the extended period of time between $T_{compromise}$ and $T_{effects\ apparent}$ provides a window of opportunity for the target state to detect and remove the malicious code, thereby fending off the attacker's use of force. The longer the logic bomb lies dormant, the more susceptible it becomes to detection by the target state and the lower the expected value it has to the attacking state as a military operation.[103] But it has already been shown that the target state has some obligation to keep the networked components of its infrastructure from being used to harm its civilian population. If the logic bomb is found, the target state must take steps to remove it, rather than knowingly place its population at risk. If it does so, then the intended effect cannot occur: the scale and effects of the whole operation do not rise to the level of an armed attack, but are merely a technological inconvenience.

There are two lines of thinking from this point. Neither one depends on the scales-and-effects doctrine, because there are no significant harmful effects to assess. On one hand, Charles Dunlap suggests that if intent is separated from capability, and if there is no discernible intent to trigger the logic bomb in the near term, then there could be reason to say that merely deploying the logic bomb would not be a use of force, even after $T_{compromise}$.[104] And this seems reasonable, since the effects that would make the cyber incursion a flagrant cyberattack did not happen. Further, the *Tallinn Manual* suggests that hostile actions that "generat[e] mere inconvenience or irritation will never" meet the threshold of being a use of force, and thus not be even a moderate cyberattack, so they cannot meet the threshold of being an armed attack.[105] Yet all that a detected and removed logic bomb produces is inconvenience and irritation.

On the other hand, placing the logic bomb *is* a kind of incursion, and it gives the aggressor state the capability, if it so chooses, to execute a fla-

[103] This also reduces the operation's likelihood of success, which runs counter to the expectation that the operation provide a definite military advantage to the attacker. *Tallinn 2.0*, Rule 100, comments 22, 23.

[104] Dunlap, "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar," 218.

[105] *Tallinn 2.0*, Rule 69, comment 9(a).

grant cyberattack. The logic bomb may be *intended* to cause physical harm at some point in the future, even if it is never triggered. If the harm that would result if the logic bomb were triggered would render it a flagrant cyberattack, and thus equivalent to an armed attack, it could then be argued that its emplacement is but one part of an extended flagrant cyberattack because it places persons and property in the target state in some kind of danger.[106] Further, even if the logic bomb were to be detected and removed before it could be triggered, this removal does not change the invasive and potentially harmful character of the attack. It still "qualifies as an attack if, absent such defences, it would have been likely to cause the requisite consequences."[107] On this account the target state may have just cause to respond with a use of force at $T_{attack\ launch}$, even though it may not know about the attack until $T_{effects\ apparent}$. The first line of thinking gives priority to the longer temporal distance and the scale and effects of the minimal realized harm, while the second gives priority to the intended and indirect effects of the causal chain, even though they would not follow (temporally) immediately from the initial emplacement.

The *Tallinn Manual* is not being contradictory here. Rather, it shows how complex the deliberative process is, and that the careful assessment of each just-cause criterion will mean that some of them point in different directions. But I think the second line of thinking—that unrealized but intended effects that would be equivalent to an armed attack had they come about—cannot, on its own, satisfy the just-cause criteria for a nocuous response since the cyberattack has been thwarted. While there would be a demonstrably close causal connection between the placement of a logic bomb (at $T_{compromise}$) and its intended effects (at a non-existent $T_{effects\ apparent}$), the temporal distance between the two negates the permissibility of a nocuous response if the intended harm does not arise. In other words, the violation of sovereignty may be just cause for a forceful response but the remaining just-cause criteria for a nocuous response cannot all be satisfied, so any response would be limited to at most a moderate one that will not cause physical harm.

[106]The commentary on AP I, Art. 49, in considering whether laying land or sea mines could be considered an armed attack, noted, "The general feeling was that there is an attack whenever a person is endangered by a mine laid." *Commentary on the Additional Protocols*, ¶1881. The discussion on land and sea mines can, by analogy, extend to logic bombs or other aggressive cyberoperations. *Tallinn 2.0*, Rule 92, comment 16.

[107]*Tallinn 2.0*, Rule 92, comment 17.

First, note that all of the foregoing depends on interpreting $T_{\textit{effects apparent}}$ as the time when harmful effects become manifest. The second line of reasoning may seem to be stronger if $T_{\textit{effects apparent}}$ is understood as the time when the *potential* extent of the effects become apparent, regardless of their actual occurrence. But this interpretation turns the question into one of using proportionate means to eliminate the threat of those effects occurring, not the right to a nocuous response to real harm. Rather than leave the interpretation of $T_{\textit{effects apparent}}$ open, I will grant that being aware of the possibility of harmful effects occurring and being aware of actual harmful effects are two different things, and propose $T_{\textit{harm occurring}}$ as the point in time when physical harm, understood as loss of life or damage to property, begins.

Now consider this analogy. Someone places a bomb in a subway station ($T_{\textit{attack launch}}$ and $T_{\textit{compromise}}$). The bomb is not hidden. It is in a clear, unlocked case on the counter of the lottery kiosk, and the time to detonation is displayed for anyone to see if they know where to look. Further, the instructions for defusing the bomb are attached to the case, and the person staffing the kiosk gladly points them out to anyone who asks. When the police notice the bomb ($T_{\textit{effects apparent}}$), the display reads 43 days, 16 hours, 37 minutes, and 19 seconds. They easily disarm the bomb, and the intended damage does not occur (there is no $T_{\textit{harm occurring}}$). The scale-and-effects doctrine suggests that since the intended effects did not occur, the actual outcome was an inconvenience. Even if the placement of the bomb can be attributed to another state, a nocuous response is not justified, for the threat has been removed by non-forceful means, and a mere inconvenience is not cause for a nocuous response. This meatspace analogy to a logic bomb in the cyber realm reveals that the triggering conditions may take a long time to occur, and the longer that time, the more likely it is that the bomb can be discovered and disabled. If that happens, it does not seem that a nocuous response is justified. In both cases (and absent any other military activity against it) the target state's recourse seems to be limited to a strong diplomatic response, perhaps in conjunction with a moderate cyber response.

This analogy also suggests that additional time points will be helpful in assessing the permissibility of a forceful response. The first is the point at which the targeted state begins gathering intelligence on the source of the attack. Call this $T_{\textit{responsive intelligence collection}}$. This intelligence-gathering includes identifying, on the basis of the available evidence and to an impre-

cise but principled standard of reasonableness, who the responsible party is and whether that party can be considered an organ of a state. Only then can the target state prepare a just response against the attacking state; that preparation begins at $T_{response\ preparation}$. The response, if it is a moderate or nocuous one, is launched at $T_{response\ launch}$. The time that the original attacking state becomes aware of the response's effects does not factor into the analysis, but the time that the threat to the target state has been either neutralized by the target state or withdrawn by the attacking state is a significant milestone. $T_{attack\ withdrawn}$ identifies this point, and $T_{response\ withdrawn}$ designates the corresponding withdrawal of the target state's countermeasures against the attacking state. On this account $T_{effects\ apparent}$ will always occur unless $T_{attack\ withdrawn}$ occurs before that (leaving the target state unaware of the operation), and $T_{harm\ occurring}$, if it ever occurs, will occur no earlier than $T_{effects\ apparent}$. Some typical schematic timelines are shown in Figure 5.2; in particular, timeline (c) reflects this defused bomb scenario.

Now suppose that the bomb in the subway has been discovered ($T_{effects\ apparent}$), but police do not disarm it immediately because the detonation time is more than six weeks away. They are ordered by their government to identify who placed it ($T_{responsive\ intelligence\ collection}$). If it was placed by another state's military, then they are to let it go off ($T_{harm\ occurring}$) rather than defuse it so there will be the illusion of cause to retaliate against that other state. The scale and effects of the damage by themselves are enough to justify a use of force, including a nocuous one if necessary, to end the threat against it. However, in this case the target state did not make the minimum response necessary—defusing the bomb—to eliminate the threat (there is no $T_{attack\ withdrawn}$). The temporal distance between placing the bomb and its detonation provided ample opportunity to mitigate its effects with this minimal effort. And that is what the proportionality obligation of *jus in bello* prescribes: any response is limited in severity to what is justifiably needful to end the threat. If the target state has adequate time and means to end the threat but does not exercise that minimal effort to do so, and if the attacking state has made no other threat or use of force, then if the bomb does explode, the target state has no justification for launching a nocuous response in self-defence. A state that claims a right to a nocuous response when the obligation to use a minimum effective response has gone neglected is making a brazen attempt to avoid the state responsibility of protecting its citizens from harm.

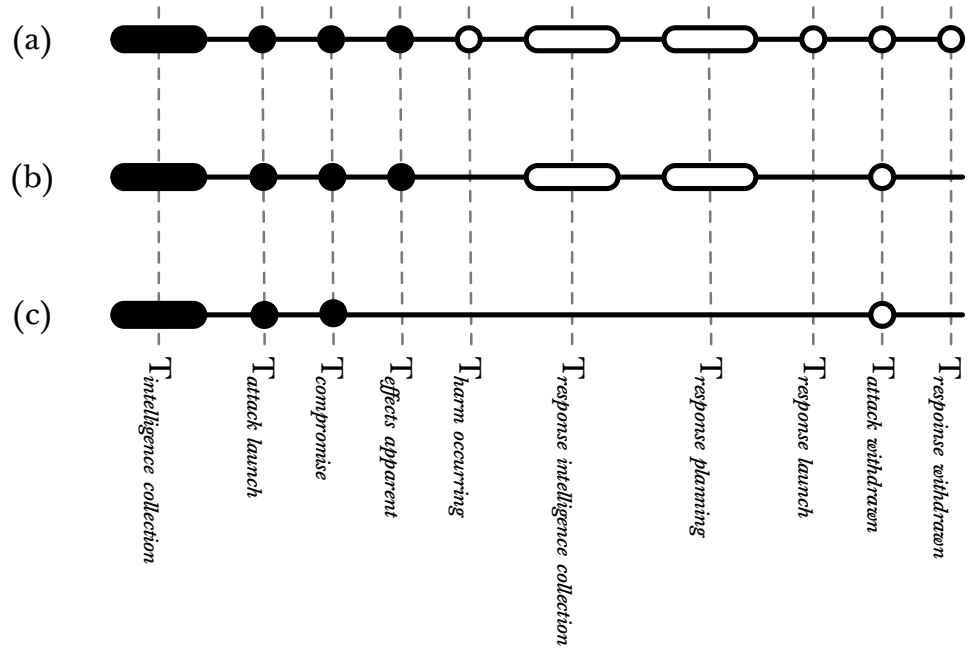


Figure 5.2: Attack-and-response schematic timelines. The timelines show the order of events and not the amount of time between them. The solid markers for $T_{\textit{intelligence collection}}$, $T_{\textit{attack launch}}$, $T_{\textit{compromise}}$, and $T_{\textit{effects apparent}}$ signify the events that are presented in the Owens report[a] (Figure 5.1), while the open markers signify the events introduced in this analysis. Timeline (a) shows all the events described in the text in their typical order. Timeline (b) illustrates the order of events where the target state recognizes the potential for harm, but that harm does not take place. Because $T_{\textit{harm occurring}}$ does not occur, a use of force is not justified, so $T_{\textit{response launch}}$ ought not occur, and withdrawing the countermeasures at $T_{\textit{response withdrawn}}$ will not be required. Timeline (c) represents the withdrawal of a a logic bomb from a compromised system before the target state becomes aware of it. The threat ends at $T_{\textit{attack withdrawn}}$ with no involvement from the target state.

[a] Owens report, 89–90.

By analogy, if the target state discovers a dormant logic bomb in a critical C2 system and has the knowledge and means to remove it, any intentional failure to do so negates the right of a forceful response in self-defence. The state did not avail itself of the least forceful means of self-defence. So even if there is a short *causal* connection between the placement of a bomb (logic or otherwise) and its effects, provided that the target state has the means and ample time to disable it, the *temporal* distance between the placement and the anticipated effects negate whatever just cause the target state may have otherwise had for even a moderate response. Thus temporal and causal distance need to be considered separately in determining whether a forceful response can be justified.[108] None of this diminishes the attacking state's responsibility for any harm that does occur. The key point is that the target state loses its right to a forceful response if it deliberately fails to satisfy its obligation to protect its citizens from the harms of a flagrant cyberattack.

Second, the target state has to identify the state that placed the logic bomb before it can make any kind of response. However, identifying the responsible party ($T_{responsive\ intelligence\ collection}$) is both time- and resource-intensive. There may be a clearly evident and close causal connection between the first stage of the attack at $T_{attack\ launch}$ and its realized effects at $T_{harm\ occurring}$, and that close connection would weigh in favour of a forceful response (including a nocuous one if the attack's effects support it). But it would be unjust to respond against the wrong party. If there is enough temporal distance between $T_{harm\ occurring}$ and identifying the responsible party at the end of $T_{responsive\ intelligence\ collection}$ that the attacking state has ceased its activity, that distance may also negate the right to respond with a nocuous use of force. Any permissible response is limited to what is needful to end the threat, and where there is no imminent or ongoing harm, there is no longer a threat to address. A less forceful response, perhaps involving a moderate cyber response and a diplomatic demands for reparations and to cease and desist from further aggressive cyberoperations, would be permissible and appropriate until and unless the threat is renewed.

Third, in extreme cases the effects of an armed attack may not be produced until long after the larger conflict is settled. Suppose a piece of ordnance from a long-past war explodes, causing damage equivalent to what

[108] This analogy was first developed in a conversation with David DeVidi.

an armed attack would produce in an active conflict.[109] The international community would not consider such an incident to be an armed attack, for no current government is responsible for its placement (that is, there is $T_{harm\ occurring}$ without a relevant $T_{intelligence\ collection}$ and $T_{attack\ launch}$). The responsible state may not even exist when this damage occurs. If the earlier conflict has been concluded well, then any permissible forceful response or warfaring activity had already taken place, and settlement for damages had already been negotiated as part of ending the armed conflict. This temporal distance mitigates the right, and has probably already eliminated the desire or ability, to make a moderate or nocuous response, even though there is a close causal connection between the device's placement and its detonation. The same scenario may occur with a logic bomb. A logic bomb placed but forgotten by one state may be triggered after hostilities have ceased. The considerations around old ordnance are analogous to those of leftover artefacts from aggressive cyberoperations. There is no need, and no justification, for an nocuous or even moderate response when there is a negotiated settlement in place to address any damage and reparations.

Each of these cases in its own way demonstrates why causal closeness and the scale and effects of any harm caused or intended by an aggressive cyberoperation are not sufficient to justify an armed response from the target state, particularly when the intended harm has not occurred. The temporal aspect must be considered independently of these criteria. Depending on the context, and how the target state makes use of any time it might have to mitigate the harm, the time between the placement of malicious software and the production of its harmful effects weighs heavily against the permissibility of any nocuous response.

5.7 Conclusion

The scale-and-effects doctrine provides some guidance on assessing the harm wreaked by aggressive cyberoperations. However, the guidance is limited to comparing the effects to those of conventional attacks as they unfold over a short period of time. Cyberoperations may take place over an extended period of time, and the scale-and-effects doctrine is intended to apply in the short term. Cyberoperations that cause economic harm or undermine the

[109] I thank Shelly Jordan for the question on how to address this kind of situation.

institutions necessary for a state to function are not comparable to conventional armed attacks in terms of effects since there is no physical harm to assess. The scale-and-effects doctrine with respect to just cause do not support a nocuous response. If the scale-and-effects doctrine is a part of assessing the harm done by an aggressive cyberoperation, it must be generalized to incorporate the harm done by violations of sovereignty or economic disruption in a way that manages the incommensurability of the various types of harms aggressive cyberoperations can produce. Classifying cyberattacks as moderate or flagrant, and permissible responses as non-forceful, moderate, or nocuous, facilitates this. A flagrant cyberattack may give just cause for a nocuous response by cyber or kinetic means; a moderate cyberattack would, at most, give cause for a moderate cyber response.

Further, an extended temporal distance between them provides the target state an opportunity to neutralize the threat before any harm may occur. This diminishes the target state's ability to claim the right to a nocuous response in self-defence. The target state's recourse is limited to what is needful to end any threat against it. Thus the two assessment criteria of causal *directness* and temporal *immediacy* set out in the *Tallinn Manual* must be assessed separately when determining whether a flagrant cyberattack has taken place and considering what kind of response may be justified. I have also shown that at least one analogous scenario can arise in meatspace, so the problems associated with immediacy and directness are not unique to cyberwarfare.

Chapter 6

Cyber *jus in bello*: the problem of protecting data and cyberobjects

6.1 Artefacts and records

The preceding chapters have looked at cyberwarfare and its analogues with conventional kinetic warfare. Cyberwarfare also opens up what has been called a "fifth battlespace,"[1] "the space of a myriad of electrical and logical connections"[2] containing not only the computing and network infrastructure of interest to a state, but also the software and data stored and used within that cyber infrastructure. The data objects of cyberspace can themselves be damaged or destroyed by a cyberattack without causing physical harm to the equipment. On a very narrow interpretation of harm under the laws of armed conflict, if one state targets another with a cyberattack that only destroys information but not hardware, there is no physical damage,

[1] Paul Cornish et al., *On Cyber Warfare*, technical report (The Royal Institute of International Affairs, October 2010), viii, http://kms2.isn.ethz.ch/serviceengine/Files/ESDP/124065/ipublicationdocument_singledocument/d922df2d-c90f-4fa6-978a-dc27940df964/en/17817_r1110_cyberwarfare.pdf. The first four are, in order of development, land, sea, air, and space.

[2] Stephen J. Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains," in Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy and National Research Council [USA], *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 109.

and therefore no measurable harm.[3] Under this interpretation, data stored in digital form is, for the most part, not protected. But the destruction of data can still be a harm to the target state, and even humanity writ large, if data objects related to the provision and exercise of human rights are destroyed by a cyberattack. It seems plausible, then, that at least some data objects that exist only in cyberspace merit some kind of protection just as certain physical objects are protected under international law. However, since it is the data that matters (a point recognized by the Shanghai Cooperation Agreement[4]), and not just the medium, any protection extended to tangible data objects should extend to those that exist in intangible form. In this chapter I will argue in support of the minority position expressed in the commentary on Rule 100 of *Tallinn 2.0* that "for the purposes of targeting, certain data should be regarded as an object" and have the benefit of protection from attack during times of armed conflict.[5]

There are two significant classes of objects that document and perpetuate a people's distinct identity and are particularly vulnerable to destruction in an armed conflict: their cultural objects and their civil records. Cultural objects are things similar to the objects on the various lists of human-built wonders of the world: the Great Pyramid at Giza in Egypt, the Taj Mahal in India, the Panama Canal, the Buddhas of Bamiyan in Afghanistan. Archaeological objects such as old scrolls and inscriptions, archaic tools, religious icons and idols, and other artefacts from earlier cultures also count as cultural objects. Works of art, including written works, may fall into this category as well, depending on their significance or rarity. These are part of the history of human cultures, markers of where peoples travelled, worked, settled, created, and fought. While these help record the history of peoples and communities, the comparatively mundane civil records track the socially significant activities of individual persons. These civil records include property deeds, tax receipts, census returns, and vital data such as births, marriages, and deaths. Where these records exist, they can be used to associate individual persons with particular peoples and cultures.

These artefacts and records in their original form are tangible. They can be seen and touched. We can read some of them; we can make images of all

[3] *Tallinn 2.0*, Rule 100, comment 6.

[4] Shanghai Cooperation Agreement, Annex 1 ("information security"); Annex 2, ¶5.

[5] *Tallinn 2.0*, Rule 100, comment 7. The rule begins, "Civilian objects are all objects that are not military objectives."

of them. Some of them (for example, musical scores) represent something else (sounds) and need a way of converting that representation to something that can be perceived by human senses (musicians and instruments). Digital technology, in a way similar to a musical score, allows artists to represent works in digital formats, but these formats need their analogues to the musicians to convert those works into perceptible form. Digital objects themselves are not tangible, but the various kinds of media containing those representations are. The cultural value of works of art created in digital form is not bound up in the storage medium—a physical artefact—but in the content stored in the medium.[6]

Our societies also create digital civil records. The compactness of digital representations makes them less costly (at least with respect to time and space) to store, access, copy, and transport records than paper-based representations (which was also a move from more awkward representations). Governments are also converting older records to digital form, whether they be digital images or data transcriptions made from the original paper records. These digital information objects are also indirectly accessible by humans. Like digital works of art, the information has to be transformed from the stored representation to something that can be readily perceived by humans. The medium itself is not the chronicle of persons' activities, but the information represented on it is. Cultural objects and civil records, two testaments to the cultural and societal history of humanity, thus have significance as intangible digital objects, and not just as tangible physical objects.

After the Second World War many states adopted the 1954 Hague Convention for the Protection of Cultural Property in the Event of an Armed Conflict (Cultural Property Convention) to protect cultural heritage from being destroyed in war.[7] The Cultural Property Convention recognizes that

[6] Perhaps the rarity of a particular kind of storage medium makes it more significant. For example, clay tablets inscribed with cuneiform lettering may currently be of more historical and cultural value than a Microsoft Windows 2000 installation disc, but when there is only one of those installation discs remaining, that particular disc might be treated with reverential care to preserve the abstract machinery (software) encoded on it.

[7] United Nations Educational, Scientific and Cultural Organization (UNESCO), Convention for the Protection of Cultural Property in the Event of Armed Conflict, The Hague, May 14, 1954, 249 UNTS 215, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2A07EB0EAA5CECACC12563CD002D6BC8/FULLTEXT/IHL-60-EN.pdf (hereafter cited as Cultural Property Convention).

objects designated as having cultural significance are not just records of particular cultures, but of humanity as a whole, and the destruction of these cultural objects diminishes human culture globally.[8] However, neither the Cultural Property Convention nor its two protocols[9] make explicit reference to the civil historical data such as taxation, property, and vital records concerning births, marriages, and deaths. I will argue that these civil records merit the same protection as other cultural objects, and that their protection is expected under the Cultural Property Convention. I will further argue that digital objects, including works of art and historical data, also merit specific protection from attacks, including cyberattacks.

6.2 Inadequacy of current protections

Cultural property

The Cultural Property Convention defines cultural property this way:

> (a) movable or immovable property of great importance to the cultural heritage of every people, such as monuments of architecture, art or history, whether religious or secular; archaeological sites; groups of buildings which, as a whole, are of historical or artistic interest; works of art; manuscripts, books and other objects of artistic, historical or archaeological interest; as well as scientific collections and important collections of books or archives or of reproductions of the property defined above;

[8] Cultural Property Convention, preamble.

[9] United Nations Educational, Scientific and Cultural Organization (UNESCO), Protocol for the Protection of Cultural Property in the Event of Armed Conflict, The Hague, May 14, 1954, 249 UNTS 358, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/79B801B4D23AEA95C12563CD002D6BE3/FULLTEXT/IHL-61-EN.pdf (hereafter cited as Cultural Property Protocol (1954)); United Nations Educational, Scientific and Cultural Organization (UNESCO), Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict, The Hague, March 26, 1999, 2253 UNTS 172, accessed April 17, 2017, http://unesdoc.unesco.org/images/0013/001306/130696eo.pdf (hereafter cited as Cultural Propterty Protocol (1999)).

(b) buildings whose main and effective purpose is to preserve or exhibit the movable cultural property defined in sub-paragraph (a) such as museums, large libraries and depositories of archives, and refuges intended to shelter, in the event of armed conflict, the movable cultural property defined in sub-paragraph (a);

(c) centers containing a large amount of cultural property as defined in sub-paragraphs (a) and (b), to be known as 'centers containing monuments'.[10]

This definition is aimed at preserving the heritage of culture writ large, including both those cultures that are no longer extant (and so no longer have a stake in any conflict between peoples) and elements of the various cultures that are present now. It also protects the record of human discovery and expression, both past and present. What it does not explicitly protect is information about *individuals* who make up a distinct people with its own cultural heritage. International laws of armed conflict are meant to preserve some of the rights of non-combatants as persons, but it does not grant explicit protection to the storage facilities that contain the birth or naturalization records that document a person's citizenship—records that are required in order to satisfy some rights obligations and to extend other rights, privileges, and duties. If the Cultural Property Convention granted explicit protection to these kinds of records, it could also serve as a convention that preserves the distinctiveness of existing cultures, not just their cultural property.

This notion of cultural distinctiveness is vague, and attempts to define it are often politically charged. It includes, to some extent, language, religion, clothing, food and drink, and artistic expression[11]—the stuff that outsiders can learn and embrace for themselves. It may include some notion of race (as fraught as that notion is) or a collective identity forged by history, partic-

[10] Cultural Property Convention, Art. 1.

[11] United Nations Educational, Scientific and Cultural Organization (UNESCO), Convention for the Safeguarding of the Intangible Cultural Heritage, Paris, October 17, 2003, Art 2(2), accessed March 4, 2021, `https://ich.unesco.org/en/convention` (hereafter cited as CICH); Sarah Song, "The Subject of Multiculturalism: Culture, Religion, Language, Ethnicity, Nationality, and Race?," chap. 10 in *New Waves in Political Philosophy* (Basingstoke, UK: Palgrave MacMillan, 2009), 178.

ularly through struggles to survive as a distinct group[12]—something that can be used to distinguish members of a cultural group from those outside of it. This distinctiveness is sustained in part by each cultural group's institutions, whether they be formally organized or informally preserved by the passing along of traditions from one generation to the next. One one hand, these institutions are part of the life of the members of the cultural group, both within their local community and in connection with the group's dispersed communities around the world. It may not be a stretch to say that the state of these institutions are reflections of the strength of the cultural group's distinctiveness, for if these institutions cease to exist, then the community that once sustained them no longer value at least the community aspect of cultural distinctiveness. On the other hand, some of these institutions are the keepers of cultural artefacts and historical documents, the very things that are evidence of the culture's distinctiveness. Moreover, those documents may also be records of the lives and identities of its members. The more that these institutions maintain records that provide evidence of the distinctive elements of the culture and the identity of its members, the greater the threat to maintaining the distinctiveness of that culture by destroying its records, collective memories, and traditions. If these history-keeping institutions devolve or dissolve as a cultural group loses its distinctiveness, the evidentiary record of that culture's existence as part of humanity's cultural heritage is at risk.

The records and artefacts of dead cultures have historical significance, but there is no expectation that the cultural practices themselves (particularly religious ones involving mutilation or sacrifice of living beings, or the renewing of hostilities against an adversarial cultural group) be preserved. These records and artefacts are the things that the Cultural Property Convention has in view. It does not say anything about preserving the *practices* of existing cultural groups. However, the records and artefacts of currently-existing cultural groups are also part of humanity's cultural heritage. These records and artefacts can support claims for personal and communal rights of some sort, whether that be the use of a language, the (peaceable) practice of religion, residency in a particular geographical area, some kind of political autonomy, or a combination of these. Moreover, the United Na-

[12] Song, "The Subject of Multiculturalism: Culture, Religion, Language, Ethnicity, Nationality, and Race?," 178.

tions, through its ICCPR, has endorsed the rights for members of existing minority cultural groups, "in community with the other members of their group, to enjoy their own culture, to profess and practise their own religion, or to use their own language."[13] However, as Will Kymlicka notes, the UN and other international organizations have not given much guidance on how these rights should work,[14] depending on the historical relationship each particular cultural group has with the state and territory in which it is situated.[15] He notes two distinct cases: mass immigration (for example, the many refugees from Syria that came to Canada around 2015) and established minorities (for example, Indigenous peoples living within Canada's borders). Groups in the former category appear to have little room to replicate their formal cultural institutions in their new state, though (at least in the short term) they can usually preserve their language, practise their religion, and promote their distinctive forms of artistic expression. Groups in the second category have a continuing presence within the territory of their governing state. While these groups may not enjoy what Kymlicka calls "national cultural autonomy,"[16] the history of that culture—and perhaps records of individual persons—as preserved by cultural institutions may support a claim to formal recognition of their distinctive culture within the state. This second category is the one relevant to my argument.

If cultures are preserved through their formal and informal institutions, then they are put at risk by undermining those institutions.[17] For example, forbidding the use of a cultural language, such as Indigenous languages in Canada's residential schools, hinders communication between the generations that used the language and those who were denied the opportunity to learn it. In 1916, the destruction of Armenian Christian churches—which

[13]ICCPR, Art. 27.

[14]Will Kymlicka, "Multiculturalism and Minority Rights: West and East," *Journal on Ethnopolitics and Minority Issues in Europe* 3, no. 4 (2002): 2–3.

[15]Will Kymlicka, "National Cultural Autonomy and International Minority Rights Norms," *Ethnopolitics* 6, no. 3 (September 2007): 381.

[16]Kymlicka, 382.

[17]Raphael Lemkin, "Genocide as a Crime under International Law" (American Jewish History Society, manuscript collection P-154, Raphael Lemkin collection, box 6, folder 2, 1948–51), 2, accessed February 21, 2019, `http://digital.cjh.org:80/R/-?func=dbin-jump-full&object_id=398972&silo_library=GEN01`. Here Lemkin coins the term *cultural genocide* to describe the destruction of the cultural and institutional expressions of a distinctive culture.

were also repositories of vital records—"resulted in the erasure of of almost all Armenian group life in Turkey."[18] Removing the institutional record of a culture's history eliminates the possibility of ever recovering the language and other cultural practices as anything more than a historical curiosity. Conversely, any surviving records and artefacts may support a right for displaced persons to return to their homeland after the threat to their safety has ended, and participate as full members of a state's society.

The institutions that harbour the artefacts and records of a distinct culture are among the marks of a political community. They also serve as an authority in the lives of that community's members. When this distinct culture and its internal politics generate conflict within the larger state, that culture may be at risk. The perceived offence need not be an attempt to exercise greater autonomy from the state; sometimes just existing as a distinct group is enough to foment discontent within the larger population. This can lead to restrictions on not only practising cultural activities, but also on access to government services, public spaces, shops, banks, schools, and jobs. This is aggravated when there is a long-standing grudge against another cultural group. Where this conflict has erupted in violence, extremists will not be satisfied with killing everyone who claims to be a member of the notional enemy. They will want to purge as much of that group's history from human memory as they can. This serves two purposes: to deny recognizing a revived culture as a legitimate one that merits protection, and to avoid charges of genocide. If there is no record of persons ever belonging to that cultural group, it is difficult for a prosecution to gather evidence to sustain the charge of genocide. This gives reason enough to extend protection to civil records—no matter where they are stored—concerning individual persons. If the Cultural Property Convention does this, then the international community has another way to identify and prosecute charges of ethnic cleansing and genocide. All it takes is to clarify what is meant by *historical interest* or *archive*.

[18] Peter Balakian, "Raphael Lemkin, Cultural Destruction, and the Armenian Genocide," *Holocaust and Genocide Studies* 27, no. 1 (Spring 2013): 65.

The destruction of civil records can cause another set of harms. Think of a person who loses a wallet containing all of their recognized personal identification. Without that identification, the person has no easy access to government services, financial services, or perhaps even access to housing and employment. They have to go through an extended process to verify their identity and replace the documents. But if the civil records that corroborate the documents carried by the person are inaccessible, there is no way for the person to avail themselves of their rights as a member of that society. I explore specific examples of this later in this chapter.

However, civil records serve another purpose: the functioning of society itself, and not just the individuals within it. For example, if the statistical information from the most recent census is destroyed, there would be no current social data by which to evaluate public policies, so government would become more hit-and-miss than it is even with good data.[19] If business and income tax records are destroyed, it would impair the government's ability to collect revenue and to provide public goods and services. This kind of government instability can undermine a state's sovereignty, and in extreme or prolonged cases even threaten its existence. The follow-on harm to members of society could include the inability to enjoy their basic rights under international declarations and covenants if the state can no longer safeguard or facilitate that enjoyment. It is not a stretch to propose that for a state to satisfy its existing obligations under international human rights rules, the data it needs to fulfil those obligations should enjoy protected status in times of armed conflict—a status that is not explicitly provided for under the international laws of armed conflict, but is nonetheless supported by international agreements such as the Cultural Property Convention[20] and AP I.[21]

[19] For example, the replacement of Canada's mandatory long-form census with a voluntary household survey in 2011 resulted in misleading or inconsistent statistics with respect to immigration and income. Ontario Council of University Libraries (OCUL), "Cancellation of the Mandatory Long-Form Census—Background and Impact," January 5, 2015, accessed March 4, 2021, `https://ocul.on.ca/node/3400`. This could lead to an underprovision of relevant social services and misguided changes in government policy.

[20] Cultural Property Convention, Art. 18, 19.

[21] AP I, Art. 53(a).

6.3 Physical objects and replicas

The cultural property described in the Cultural Property Convention exists in concrete form, not as a representation in some other kind of media. It is, for lack of better terms, enduring or persistent. Further, many of these culturally significant items are typically original and unique. These items also vary in size, from small archaeological items such as arrowheads and iron nails, to large sites like the Pyramid Fields from Giza to Dahshur in Egypt, to entire cities like Bath in England. Many of these are not readily reproducible; their loss would diminish the understanding of both human and natural history. Items such as books, manuscripts, recordings, and some works of art are less durable, but more readily reproduced. If faithful reproductions of these cultural artefacts exist, the loss of the original does not diminish the record of human discovery, creativity, and society as much as the destruction of a unique object would. The content and expression of the original is preserved in each replica, even though some of the fine details may be lost.[22] In many cases each replica will be indistinguishable from the others, so any one will do for the purposes of preservation.[23] For example, the copies of any Canadian publication required to be deposited with Library and Archives Canada[24] do not have to be the first one or two from the production run. The Cultural Property Convention extends protection to archival reproductions of cultural property, regardless of the media in which those reproductions are made.[25]

[22] For example, a digital compact disc recording of a jazz trio will encode enough of the sound to satisfy the casual listener, but a listener highly attuned to the continuous form of sound waves may notice the small discontinuities the digital sampling process introduces. A detailed photograph of an oil painting will give a representation of the original without reproducing the texture of the strokes, even though it will provide visual cues about them. The same level of photographic detail will not capture the shape of a sculpture, but a three-dimensional model could.

[23] *Tallinn 2.0*, Rule 142, comment 6.

[24] Library and Archives Canada, "Legal Deposit," February 22, 2018, accessed April 19, 2018, `https://www.bac-lac.gc.ca/eng/services/legal-deposit/Pages/legal-deposit.aspx`.

[25] Cultural Property Convention, Art. 1(a).

6.4 Data objects

I have already noted that some of the objects stored in archives are not works of intellectual or creative labour. They are data objects: records of individual events and transactions used in part to manage the affairs of a particular state or society.[26] These records document (among other things) births, deaths, marriages, immigration, citizenship, military or other civic service, property ownership, taxation, and legal proceedings. While cultural artefacts trace the development of peoples and cultures,[27] these data objects trace the activity of persons and states. They are of significance to the operation of a state.[28]

Data objects often describe relationships. For example, one way of viewing a contract is as a data object describing the rights and obligations of the contracting parties with respect to each other. The interpretation of these terms may be guided by descriptions in other data objects such as legal statutes and court judgements, which themselves grant rights and establish obligations. Taxation records establish whether a party has contributed their share to the government. Census returns and birth, death, and mar-

[26] *Society* is not a synonym for *culture*. A society may include many cultures, and a culture may be represented in many societies.

[27] *Peoples* and *cultures* are also distinguished. International law grants the right to self-determination to peoples, but not to all who claim a particular cultural heritage. Members of "ethnic, religious, or linguistic minorities" living within a people's territory "are merely entitled to enjoy their own culture" within that territory. *Commentary on the Additional Protocols*, ¶1106.

[28] The International Council on Archives (ICA) describes archives and their importance this way: "Archives constitute the memory of nations and societies, shape their identity and are a cornerstone of the information society. By providing evidence of activities and decisions they provide continuity to organizations and justification of their rights, as well as those of individuals and states. By guaranteeing citizens' right of access to official information and to knowledge of their history, archives are fundamental to democracy, accountability and good governance." International Council on Archives (ICA), *Constitution*, August 24, 2012, preamble, accessed April 21, 2018, `https://www.ica.org/sites/default/files/constitution_2012_en_final_2016_visual_identity.pdf`. ICA is one of the founding organizations of the Blue Shield, the international association "committed to the protection of the world's cultural property . . . in the event of armed conflict, natural- or human-made disaster" and advocating for adoption and implementation of the Cultural Property Convention. Blue Shield, *Amendment to the Articles of Association: Association of National Committees of the Blue Shield*, Amsterdam, NL, April 6, 2015, Art. 2.1, 2.3, accessed March 5, 2021, `https://theblueshield.org/wp-content/uploads/2018/06/statute-Amendments_BSI_2016.pdf`.

riage records capture the relationships of natural persons to each other. Military service records chronicle other kinds of relationships between a persons and their government, persons and locations, and persons with other persons within a command structure or as comrades-in-arms. If these data objects are lost and cannot be recovered, it is not just the state that loses this bit of its recorded history and collective memory. All of the parties identified in these records lose the evidence that supports what each of them remembers. Some contextual information about their lives (for fictional persons, existence) is lost—and that loss may affect how those parties can operate in the future. Suppose that a person is the parent to a young child. If every copy of the record of that child's birth is lost, then the parent cannot claim social benefits meant to support that child because the documentation of the parent-child relationship no longer exists.[29] Regardless of the medium in which these relationships and events are recorded (wooden tally sticks, paper, microform, digital), they have to be stored in some kind of archival repository so those who need to consult the records have ready access to them. A civil archive, then, contains the institutional memory of both the state and the cultures that it hosts, and in so doing preserves a connection to the past.

There is no objective way to identify distinct peoples within a population.[30] In a way, what establishes a group as a people is that group's desire to live as a distinct people because members of that group share a common history and one or more other identifying elements: land, language, culture, and ethnicity.[31] There must also be "something that separates them from other peoples"[32] that reasonably allows them to maintain that distinction. However, a people is not equivalent to a state under international law. A state may contain many peoples; a people may be dispersed among many states. When conflict arises there is a desire to establish a different order, and that sometimes involves weakening or eliminating a distinct people. One way to do that is to destroy objects that help that people maintain its

[29] Presumably there would be some way to make a solemn affirmation of the relationship, and that would serve as a proxy for the original record, but this is a long and complex process requiring more testimonial evidence than the original record of birth did.

[30] *Commentary on the Additional Protocols*, ¶1103.

[31] *Commentary on the Additional Protocols*, ¶1103.

[32] *Commentary on the Additional Protocols*, ¶1103.

distinctiveness, a process now called "cultural cleansing."[33] One example of such cultural cleansing is the Sovietization of the Baltic states: outlawing the local language, removing cultural artefacts, and forcibly resettling residents in other areas of the Soviet Union, while imposing a Russified culture bolstered by relocating ethnic Russians to the Baltic republics. When an independent Estonia removed a Stalin-era statue in April 2007, ethnic Russians protested for days afterward—but not ethnic Estonians.[34] These protests were followed by Russia's DDOS attack on Estonia's Internet services (Chapter 3).

The institutional memory of a culture is part of its heritage. It is of cultural significance, at least on par with its arts, artefacts, and structural ruins, because it captures some of the history of that culture. Because these records are culturally significant and a part of the shared history of humanity, they are candidates for protection under the Cultural Property Convention. Further, the Blue Shield claims that the definition of *cultural property* in the Cultural Property Convention "has the flexibility to include new forms of CP [cultural property] that were of unseen importance or were unimagined in 1954, for example, film archives and digital archives and information."[35] Yet contemporary civil records, those relevant to contemporary cultures and governance of existing societies, and which will become incontrovertibly historical at some indefinite time, are not explicitly protected under the laws of armed conflict. These contemporary civil records are a part of contemporary institutional memory, and will form a part of the shared history of humanity. Therefore they should also have some kind of formal protection from wilful damage during times of armed conflict to facilitate the preservation

[33] UNESCO, qtd. in Megan Williams, "'Dignity itself': Saving World Heritage Sites from 'Cultural Cleansing' Won't Be Easy," *CBC News*, March 31, 2017, accessed March 31, 2017, http://www.cbc.ca/news/world/saving-culture-g7-megan-williams-1.4048707.

[34] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007, accessed September 10, 2020, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[35] Blue Shield, "Defining Cultural Heritage and Cultural Property," February 11, 2020, accessed March 5, 2021, https://theblueshield.org/defining-cultural-heritage-and-cultural-property/. Just as the Red Cross is the organization dedicated to implementing the Geneva Conventions, "[t]he Blue Shield is the cultural equivalent of the Red Cross" with respect to the Cultural Property Convention. Blue Shield, "Who We Are," February 11, 2020, accessed March 5, 2021, https://theblueshield.org/about-us/what-is-blue-shield/.

of contemporary cultures—even majority ones.

The digitization of civil records opens the door for potentially destabilizing havoc from the cyber domain. It has already been established that voter records in Illinois were accessed by parties with (at least) the tacit approval of Russian political leadership.[36] While these particular records were not altered, it is a small step from accessing them to changing them. (Such an alteration would be one instance of a cyberattack with delayed effects, as discussed in Chapter 5. A record-changing cyberattack executed after the close of voter registration would not be evident until persons attempt to cast their ballots. There may be no attack in progress at the time the harm is discovered. A like-for-like moderate cyber response against the attacker's electoral system might be seen as an impermissible reprisal or a breach of their citizens' rights to vote—assuming the attacking state has free elections. A moderate cyberattack against another target might be permissible.) This breach demonstrates the feasibility of accessing and altering states' digital civil records, and this is the concern that motivates this part of the project.

Two of the significant potential consequences of changing or deleting civil records are the undermining of self-governance and the erasure of evidence to support individuals' claims of being associated with a state or a distinctive cultural group. The first of these is more subtle and disruptive than cyberharms against infrastructure such as bringing down parts of the electrical grid, even though neither one is, *prima facie*, a flagrant cyberattack meeting the criteria that can justify a nocuous response. Nonetheless, they disrupt the target society. Disrupting the electricity supply impedes not only the ability to do extraordinary things such as emergency surgery, but also the ability to do mundane things such as heating a frozen meal. This weakens the social fabric as people recognize that they have less control over their circumstances than they want. However, changing voting records un-

[36] CBS Chicago, "Illinois Election Chief to Testify at Senate Panel on Russian Hacking," June 21, 2017, accessed February 25, 2019, https://chicago.cbslocal.com/2017/06/21/illinois-state-board-of-elections-russian-hacking-senate-intelligence-committee/; Garcia and O'Connell, "Illinois Elections Board 'Very Likely' Named in Mueller Indictment of Russian Hackers, Officials Say." This does not include accessing private email exchanged by members of the Democratic Party's campaign or the social engineering that poisoned any hope of meaningful socio-political discourse, activity described in Chad Day and Eric Tucker, "Court Records Reveal a Mueller Report Right in Plain View," *CTV News*, February 23, 2019, accessed February 25, 2019, https://www.ctvnews.ca/world/court-records-reveal-a-mueller-report-right-in-plain-view-1.4309843.

dermines the political institutions themselves. This goes beyond the efforts to suppress voters through rigging electoral processes. Some persons who manage to register to vote will find that their registration is invalid or missing, and so not be able to exercise their right to express their political will. If this is done carefully enough, the outcome may be crafted to be an illusory misrepresentation of the will of the people. The structure and appearance of self-governance are in place, but the persons are politically incapacitated—much as they would be if they had been incapacitated by chemical or biological warfare, just without the physiological harm. Since this is not a physical threat to the lives of persons in the targeted state, it would be difficult to call such a disruptive cyberattack a flagrant one justifying an immediate nocuous response.

The second of these consequences concerns the cultural record of humanity. Civil records are also important for the preservation of peoples and cultures. One characteristic of a people is the territory inhabited by its members, even though that territory may be shared with persons from other cultures. A state governs the territory, so persons, cultures, peoples, and states stand in relation to each other through territory. The state, as part of its obligation to allow members of minority groups the freedom to enjoy their culture, must keep records of those within its borders who have the right to enjoy (and thus preserve) their culture.[37] However, in an ethnic conflict having some degree of sanction by the state's government, the state may be tempted to deny the existence of—or even destroy—the records of minority persons. If those persons' own copies of their records are not recognized as valid, they would no longer have evidence of their rights to enjoy their culture. They may also be denied the rights to any property they own within the state and the rights of citizenship. For example, at the height of conflict between Albanian and Serbian communities in Kosovo in 1998 and 1999,

> forces of the FRY [Federal Republic of Yugoslavia] and Serbia systematically seized and destroyed the personal identity documents and licences of vehicles belonging to Kosovo Albanian citizens. As Kosovo Albanians were forced from their homes and directed to Kosovo's borders, they were subjected to demands to surrender identity documents at selected points *en route* to bor-

[37] ICESCR, Art. 15(1)(a).

> der crossings into Albania and Macedonia. These actions were undertaken in order to erase any record of the deported Kosovo Albanians' presence in Kosovo and to deny them the right to return to their homes.[38]

While the seizure and destruction of those personal civil documents were not ruled to be crimes against humanity themselves, these actions were evidence of the deportation and forcible transfer of ethnic Albanians from Kosovo.[39] Seizing and destroying identity documents did not formally change the bearers' citizenship,[40] but it would have made it harder for those returning to claim their rights as citizens.[41] Even if those whose documents were seized knew that their citizenship was intact, the depersonalizing activity is still a psychological harm violating the general protection afforded civilians under the laws of armed conflict. It could also be viewed as an act intended to "spread terror among the civilian population,"[42] something also prohibited in non-international armed conflicts for states party to AP II.[43]

[38] International Criminal Tribunal for the Former Yugoslavia (ICTY), *Milutinović case* (redacted third amended joinder indictment), IT-05-87-PT D6404, June 21, 2006, ¶31, accessed March 20, 2019, http://www.icty.org/x/cases/milutinovic/ind/en/milutinovic_060621e.pdf (hereafter cited as *Milutinović* indictment). Milan Milutinović, the president of Serbia during the height of the Kosovo conflict, was acquitted of the charges of crimes against humanity, but the other five persons named in the indictment were found guilty on several counts. International Criminal Tribunal for the Former Yugoslavia (ICTY), *Milutinović case* (judgement), IT-05-87-T, February 26, 2009, vol. 3, ¶¶1207–12, accessed March 20, 2019, http://www.icty.org/x/cases/milutinovic/tjug/en/jud090226-e3of4.pdf (hereafter cited as *Milutinović* judgement). Four of those five appealed their convictions, but each of them had some guilty verdicts that survived the appeal. International Criminal Tribunal for the Former Yugoslavia (ICTY), *Milutinović case* (appeal judgement), IT-05-87-A, January 23, 2014, ¶1847, accessed March 20, 2019, http://www.icty.org/x/cases/milutinovic/acjug/en/140123.pdf (hereafter cited as *Milutinović* appeal judgement).

[39] *Milutinović* indictment, ¶¶71–73; *Milutinović* judgement, ¶40.

[40] *Milutinović* judgement, ¶1172.

[41] *Milutinović* judgement, ¶1166.

[42] AP I, Art. 51(2).

[43] AP II, Art. 4(2)(a), (d). The Socialist Federal Republic of Yugoslavia had acceded to AP II in 1979. United Nations General Assembly, Status of the Protocols Additional to the Geneva Conventions of 1949 and Relating to the Protection of Victims of Armed Conflicts, September 12, 1990, Report of the Secretary-General, A/45/454, 8, accessed March 6, 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N90/222/30/img/N9022230.pdf?OpenElement. The Federal Republic of Yugoslavia (the former socialist republics of

Personal records were not the only records seized or destroyed by the Serbian community in Kosovo. Six regional archives of the Islamic Community of Kosovo were damaged to varying degrees by Serbian forces, and many ancient Islamic manuscripts and rare books were destroyed.[44] One of the Serbian forces' last acts in Prishtina/Priština after the armistice was in place but before NATO peacekeepers arrived was to burn the central archive of the Islamic Community.[45] This archive contained records dating back more than 500 years.[46] The only remaining documentary evidence of Albanians having been present in Kosovo resided in civil archives, and these were not overlooked. Civil records

> comprising almost the entire documentary base for the orderly functioning of government and society in Kosova were removed on orders from Belgrade. Registries of births, marriages and deaths, citizenship, probate and property records, as well as judicial and police records, and the working documents of many other state institutions were either evacuated to Serbia or burned *in situ*.[47]

Serbia and Montenegro and the former autonomous regions of Vojvodina and Kosovo) was not recognized as a successor state by the international community at the time of the conflict. The parties to the conflict continued to be bound by the provisions of AP II and other treaties. United Nations General Assembly, Status of the Protocols Additional to the Geneva Conventions of 1949 and Relating to the Protection of Victims of Armed Conflicts, August 26, 1998, Report of the Secretary-General, A/53/287, 6, accessed March 6, 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/249/43/pdf/N9824943.pdf?OpenElement.

[44]These archives were located in Peja (Albanian name)/Peć (Serbian name), Gjakova/Đakovica, Skenderaj/Srbica, Gllogoc/Glogovac, Suhareka/Suva Reka, and Lipjan/Lipljan. András J. Riedlmayer, "Libraries and Archives in Kosova: A Postwar Report," *Bosnia Report*, nos. 13/14 (December 1999–February 2000), accessed March 21, 2019, http://www.bosnia.org.uk/bosrep/decfeb00/libraries.cfm. Riedlmayer was an expert witness with respect to destruction of cultural heritage (but not with respect to attribution of the damage) for several trials before the International Criminal Tribunal for the Former Yugoslavia.

[45]András J. Riedlmayer, "Crimes of War, Crimes of Peace: Destruction of Libraries during and after the Balkan Wars of the 1990s," *Library Trends* 56, no. 1 (Summer 2007): 124; Riedlmayer, "Libraries and Archives."

[46]Riedlmayer, "Crimes of War," 124.

[47]Riedlmayer, "Libraries and Archives."

NATO spokesperson Jamie Shea described this activity as "a kind of 'Orwellian' scenario of attempting to deprive a people and a culture of the sense of the past and the sense of community on which it depends."[48]

This kind of community erasure continued on after the recognized end of the Kosovo conflict. In response to violence against the Serbian community over the misreporting of circumstances around the drowning of three children of Albanian descent in Kosovo on March 17, 2004, a pro-Serbian mob destroyed the Islamic library in Belgrade.[49] "Our library is destroyed, all our records are destroyed, our seals are missing, our safe has been emptied, our computers are destroyed or stolen. As the Islamic community of Belgrade we no longer exist," lamented prayer leader Mustafa Jusufspahić.[50] His father Hamdija Jusufspahić, the interpreter of Islamic law for the community, added, "If only they had left us our computers, that way we could at least recover something."[51] The destruction of computers is important here: it shows that digital records can be just as important to a community—and just as vulnerable to destruction—as paper ones.

The aftermath of Hurricane Maria in 2017 provides a recent example of the civil havoc that arises from missing records. Many of the requests Puerto Ricans—American citizens—made for assistance to rebuild their homes were turned down because there was no record—paper or digital—of ownership.[52] There is a cultural aspect to these records not existing: local custom placed property records in the collective memory of the community. As one newspaper reported, "[o]nly 65 percent of properties in the territory are officially registered with the government. The problem is especially acute in small

[48] North Atlantic Treaty Organization (NATO), "Press Conference of the NATO Spokesman, Jamie Shea, and Air Commodore David Wilby," Transcript. March 31, 1999, accessed March 25, 2019, https://www.nato.int/kosovo/press/p990331a.htm.

[49] Riedlmayer, "Crimes of War," 128–129; Milorad Mracevich, "Anti-Muslim Violence Rocks Serbia," *Balkan Reconstruction Report*, March 22, 2004, 1, accessed March 29, 2019, https://www.ceeol.com/search/article-detail?id=1171.

[50] Mracevich, 1.

[51] Mracevich, 1.

[52] Matthew Goldstein, "Puerto Rico's Positive Business Slogans Can't Keep the Lights On," *New York Times*, March 5, 2018, accessed February 28, 2019, https://www.nytimes.com/2018/03/05/business/puerto-rico-business-maria.html; News Is My Business, "Puerto Rico Property Registry Now 100% Electronic," ed. Michelle Kantrow-Vázquez, April 1, 2016, accessed February 28, 2019, http://newsismybusiness.com/puerto-rico-property-registry-now-100-electronic/.

cities and rural areas where there's a custom of property owners not recording titles to homes,"[53] because "property is often passed among family members without paperwork."[54] Even if the records exist, there is no guarantee that their validity will be acknowledged by the government. Some persons of Hispanic origin, though born in the USA, were no longer able to receive or renew passports because some midwives who served areas along the Texas–Mexico border had issued some American birth certificates fraudulently to persons born in Mexico.[55] Since it is difficult to determine which ones were issued legitimately and which ones were not, all of the birth certificates issued by midwives in the area have been thrown into question, limiting the ability of American citizens to exercise their rights not only to freedom of movement, but also to a nationality.[56]

In Canada there is a recognition that the problem of missing or inaccurate property records merits attention. Black loyalists were granted "freedom and a farm"[57] in parts of present-day New Brunswick and Nova Scotia for service rendered to the British Empire during the American War of Independence.[58] Access to and use of the land was permitted "under tickets of location," but those tickets did not confer possession of the land.[59] In 1964

[53]Goldstein, "Puerto Rico's Positive Business Slogans Can't Keep the Lights On."

[54]Frances Robles and Jugal K. Patel, "On Hurricane Maria Anniversary, Puerto Rico Is Still in Ruins," *New York Times*, September 20, 2018, accessed February 28, 2019, https://www.nytimes.com/interactive/2018/09/20/us/puerto-rico-hurricane-maria-housing.html.

[55]Kevin Sieff, "U.S. Is Denying Passports to Americans Along the Border, Throwing Their Citizenship Into Question," *Washington Post*, September 13, 2018, accessed March 8, 2019, https://www.washingtonpost.com/world/the_americas/us-is-denying-passports-to-americans-along-the-border-throwing-their-citizenship-into-question/2018/08/29/1d630e84-a0da-11e8-a3dd-2a1991f075d5_story.html?noredirect=on. The practice of denying passports began with the George W. Bush administration, but escalated under Donald Trump's presidency.

[56]Universal Declaration, Art. 13, 15.

[57]Jessica Murphy, "Black Nova Scotians May Finally Get Title to Their Land," *BBC News*, October 8, 2017, accessed May 22, 2019, https://www.bbc.com/news/world-us-canada-41488953.

[58]Nova Scotia Archives, "African Nova Scotians in the Age of Slavery and Abolition: Black Loyalists, 1783–1792," May 2019, accessed May 22, 2019, https://novascotia.ca/archives/Africanns/results.asp?Search=&SearchList1=2&Language=English.

[59]Nova Scotia Archives, "African Nova Scotians in the Age of Slavery and Abolition: Establishment of the Negroes in Nova Scotia, Appendix 23," Transcription of portion of Minutes of Council, March 11, 1841. May 2019, accessed May 22, 2019, https://novascotia.

the provincial government introduced a process for residents to establish a claim to title,[60] but it moved slowly and stalled out. In 2017, on the advice of the UN,[61] the province announced new resources to facilitate the process.[62] Even now residents of some historically Black communities in Nova Scotia do not have clear title to the land on which they live, so the property cannot legally be sold or willed to others.[63] This work is ongoing.

Items of cultural significance may also be lost through indifference, cost management, lack of recognition of their significance in the moment, accident, or even vanity. Broadcast media is particularly susceptible to this, because transmissions can be made without being recorded in any way. However, even recorded broadcasts are vulnerable. Robin Woods, who supervised the English-language program archives at the Canadian Broadcasting Corporation (CBC) from 1959 to the early 1980s, drew attention to this in one report. The earliest recordings by the Canadian Radio Broadcasting Commission (CRBC, the forerunner to today's CBC) were, for the most part, not concerned with Canadiana or the international tumult preceding the Second World War. Rather,

> the recordings from this period reflect little but sweetness and light—God in his Heaven, King George the Fifth upon his Imperial Throne, and all right, or about to be, with the world.

---

ca/archives/africanns/archives.asp?ID=137&Transcript=1.

[60] Nova Scotia, *Land Titles Clarification Act*, RSNS c. 250, s. 1. Formerly the *Community Land Titles Act*, SNS 1964, c. 3. 1964, accessed May 22, 2019, https://nslegislature.ca/sites/default/files/legc/statutes/landtitl.htm

[61] United Nations General Assembly, Report of the Working Group of Experts on People of African Descent on Its Mission to Canada, August 16, 2017, Report, A/HRC/36/60/Add.1, Human Rights Council, ¶¶60–61, 96, accessed May 22, 2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/239/60/PDF/G1723960.pdf?OpenElement.

[62] Nova Scotia, *Government Helping Communities Get Clear Title to Land*, News release (African Nova Scotian Affairs, September 27, 2017), accessed May 22, 2019, https://novascotia.ca/news/release/?id=20170927001.

[63] It can, however, be taxed, even though it is not clear who is responsible for paying the tax. Some residents have been advised to let their properties go up for tax sale, reacquire the land by paying the taxes owing, and in so doing get clear title to the property, but this requires being informed of the pending sale. Angela Simmonds, *This Land Is Our Land: African Nova Scotian Voices from the Preston Area Speak Up*, project report (Schulich School of Law, Dalhousie University, August 19, 2014), 8–9, accessed May 22, 2019, https://nsbs.org/sites/default/files/ftp/EQ20140819_ThisLandIsOurLand_Final.pdf.

> . . . This policy in Canadian broadcasting of recording and preserving the extraordinary and ignoring the every day—the real warp and woof of the fabric of history—was to continue for many years.[64]

Even when recordings were made as a matter of course, they were not assessed for significance or managed in any way.

> [P]roducers and others . . . decided what to keep and what to destroy. This personal and unco-ordinated exercise of policy and judgment allowed full reign to vanity, carelessness, ignorance, and sheer fecklessness. . . . There is one particularly sad example of the consequences of this willy-nilly policy. In 1943 violinist Adolf Koldofsky discovered in Toronto manuscripts of seven C.P.E. Bach concertos which had been lost for two hundred years and which had never been performed in public. The manuscripts were authenticated by Wanda Landowska who came to Toronto to give the works their world premiere on the CBC. With one precious, chance exception, all recordings of this series were destroyed. The result of this carelessness is a triple loss: to musicology, to the recorded repertoire of Landowska (these were the only recordings ever made of her performance of the works), and to the CBC. We must suffer twice: the loss of the recordings and the odium of having lost them.[65]

But archiving recordings is not enough to preserve one-of-a-kind performances. Those recordings have to be stored on stable, readable media. The record of Canadian culture suffered a blow during 1967, when "a million feet of film—largely nitrate—in care of the Canadian Film Archives . . . burned in its storage area. The disaster could have been averted had the Canadian government supplied a grant . . . to transfer the film to safety stock which the CFA had requested in 1964."[66]

[64]Robin Woods, "Report on National Program Archives," *ARSC Journal* 2, nos. 2/3 (Spring–Summer 1970): 6, accessed April 1, 2019, `http://www.arsc-audio.org/journals/v2/v02n2-3p3-23.pdf`. This also demonstrates how the selection process can shape the national cultural narrative, but exploring that is outside the scope of this project.

[65]Woods, 7.

[66]Woods, 20n.

Data destruction and document invalidation are cheap and simple ways to strip persons of their rights. When the only copy of an artist's recording is destroyed, that diminishes their right to recognition as an artist and contributor to the culture.[67] When this destruction happens to an ethnic minority, that community's existence is threatened. If that community should disappear, then its cultural heritage in that territory might also be removed, opening the way for the state to craft a new national narrative. Protecting the records of persons is one way to approach the obligation to protect the cultural heritage of humanity as a whole. This draws attention to the internationally condemned practice of cultural cleansing.

Cultural cleansing by data destruction does not fit the definition of *genocide* set out in international law because it does not result in significant bodily harm to large numbers of persons belonging to an identifiable culture.[68] Nonetheless, it does strip those persons of the right to preserve and practise their culture as a means of forcing assimilation or as an inducement to emigrate. But there are other ways to bring about cultural cleansing. An admittedly contrived example is a state restricting domestic meat production to swine, prohibiting imports of all other meats, and imposing tariffs on pulses and legumes in order to make it infeasible for Muslim and Jewish

[67] ICESCR, Art. 15(1)(c). While it is a stretch to say that "the full realization of this right" is owed to the artist by the state in a positive sense, if a representation of the artist's work exists and it is of recognized cultural significance (such as Landowska's recordings were), ICESCR expects its states parties to take "steps . . . necessary for the conservation . . . and the diffusion of . . . culture." Art. 15(2).

[68] The term *genocide*

> means any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such:
>
> (a) Killing members of the group;
> (b) Causing serious bodily or mental harm to members of the group;
> (c) Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part;
> (d) Imposing measures intended to prevent births within the group;
> (e) Forcibly transferring children of the group to another group.

United Nations General Assembly, Convention on the Prevention and Punishment of the Crime of Genocide, December 9, 1948, 78 UNTS 277, Art. 2, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/1507EE9200C58C5EC12563F6005FB3E5/FULLTEXT/IHL-51-EN.pdf (hereafter cited as Genocide Convention).

persons to eat. While this is not direct starvation, such restrictions would still be intended to cause "serious . . . mental harm to members of" those groups[69]—and this kind of cultural cleansing does fall under the category of genocide. One way to view cultural cleansing is as a means of perpetrating cultural destruction, followed in increasing efficiency of expungement by ethnic cleansing (forced removal of persons), identity cleansing (as happened in Kosovo), and genocide. It is important to resist the temptation to think of these actions as a continuum in metaphoric shades of grey; the more appropriate metaphor is glossiness of black.

Data destruction can also facilitate genocide without involving cultural cleansing. If there is no civil record of a person's birth, employment, taxation, military service, education, or residence, there is no documentation of that person's existence. This also affords a state committing genocide plausible deniability for the murder of undocumented individuals. Protecting these records provides a formal and admittedly weak means of preventing genocide, but the greater value of protection comes through preserving evidence that these persons once existed and had the right to be recognized as persons equal to any other person before the law.[70] If many persons from an identifiable cultural community have no civil records to testify to their existence, and those persons are contemporaries who cannot be found alive, it may be evidence to support a claim that a genocide has taken place.

6.5 Digital objects and data integrity

None of the records described above depend on cyber infrastructure for their preservation. However, when those objects and records do have a representation in the cyber realm, the *Tallinn Manual* affirms that, when the objects and records are cultural property of some sort, then the Cultural Property Convention applies to them.[71] Cultural artefacts may even have more protection in digital form than in tangible form because they have a claim to being the intellectual property of a cultural community. Intellectual property is intangible and relies on being represented in some medium in order to

[69] Genocide Convention, Art. 2(b).

[70] ICCPR, Art. 14, 16, 26.

[71] *Tallinn 2.0*, Rule 142.

be of use.[72] In the same way that some cultural artefacts can be represented in digital form, so can the information content of civil records.[73] These digital representations are themselves objects in an abstract sense. But the ability to access and interpret these representations depends on other objects, some concrete and some abstract. The representations are stored, transmitted, and presented in human form through different pieces of equipment: storage media and access devices, networks, displays, perhaps 3-D printers. They are converted to human-accessible form through software (another abstract data object representing a machine) executed by a computing device. These digital objects, storage media, and associated equipment do not look anything like the archives or buildings that house cultural property described in the Cultural Property Convention. But if these digital objects are the sole remaining representations of these cultural or data objects, they contain the record of human culture and thus should be protected under the Cultural Property Convention.[74]

The seizure and destruction of computing equipment and records in Kosovo demonstrates the fragility of physical storage. The digitization of data objects does not make them any less vulnerable to destruction by physical means. It only concentrates the representations into a smaller physical space. Destroying the physical objects that hold these digital representations makes the information contained in those objects inaccessible. If a particular cluster of hard disk drives contains the only representation of a piece of information (say, the record of a person's birth) and the machines containing those disks are destroyed by a sledgehammer, projectile, bomb, or fire, then that information is irretrievable. It will have been made inaccessible and so, for all practical purposes, it is gone. It can be reconstructed from testimony, but as already noted, testimony about a person's identity is often not accepted, even if it comes from non-first-person sources.

---

[72] *Tallinn 2.0*, Rule 142, comment 5.

[73] This also provides the benefit of easy indexing and searching, so there is an operational efficiency to be had.

[74] While the Cultural Property Convention extends protection to reproductions, not all reproductions are of cultural importance. The loss of some reproductions does not diminish humanity's cultural heritage. Otherwise it would be against the Cultural Property Convention to damage a copy of any book, regardless of its content. However, the *last remaining readable* representation is culturally significant because its loss would diminish this heritage. *Tallinn 2.0*, Rule 142, comment 6.

While destroying storage media is one way of destroying information, alteration is another. Digital data objects, unlike paper- or microform-based ones, can be modified without leaving physical evidence of the alteration[75] (the creation of forged records notwithstanding, since they would appear to be unaltered). Digital storage systems with low-grade (or no) encryption and inadequate control over data integrity checking are vulnerable to alteration through software specifically designed for the purpose. Once a digital record is altered, it will be difficult to track the source of the alteration—if it is ever detected. The first data backup taken after the alteration will commit the change to some kind of longer-term storage, and depending on how the change is made, it can be propagated to other data systems in a matter of seconds. Older forms of archives are not prone to this kind of rapid reproduction of alterations, in part because they typically have a documented "chain of custody"[76] identifying persons or organizations responsible for the creation, modification, and safekeeping of that record. A well-managed chain-of-custody system for an archive should make it possible for any user to verify the authoritativeness of any record,[77] regardless of how its is stored.

The chain-of-custody processes around physical archives are not adequate for digital archives because of the risk of digital alteration. However, adapting and expanding chain-of-custody processes to cover digital archives is possible without requiring the conversion of physical archives to digital ones. The international scientific community worked with archival and information management specialists to specify a framework that, if implemented and followed, will provide the chain-of-custody and authentication processes needed to preserve the integrity of archived data. In 2012 this functional reference model was accepted by the International Organization for Standardization (ISO) as an international standard addressing the authenticity and

[75] National Research Council [USA], *Building an Electronic Records Archive at the National Archives and Records Administration: Recommendations for a Long-Term Strategy.*, ed. Robert F. Sproull and John Eisenberg (Washington, DC: The National Academies Press, 2005), 59. Quantum storage devices might make this kind of tampering detectable the first time the record is accessed, but current commercially-available technologies are still vulnerable, depending on how things like digests, checksums, encryption keys, and device controllers are managed.

[76] National Research Council [USA], 59.

[77] National Research Council [USA], 69.

security of digital archives,[78] though its principles apply to other archives as well. This specification is, in many ways, aspirational, but it does identify the minimal components to assure data security and integrity—provided the relevant procedures and policies are followed once they are established.

The technological aspect of data preservation is a tractable problem with many feasible solutions ranging from paper originals and duplicates to encrypted cloud-based storage with multiple hosts. In many ways, the technology is the easy part. The human aspects of data creation, storage, access, and preservation are not so neat.[79] Among other things, the administrators of an ISO-compliant archive are obliged to "ensure that the information is preserved against all reasonable contingencies, including the demise of the Archive, ensuring that it is never deleted unless allowed as part of an approved strategy. There should be no ad-hoc deletions."[80] Having adequately-trained and effective administrators to manage the available technology, data sources, processes, and user base will go a long way to providing a framework for managing data objects—digital or physical—in a way that facilitates their preservation. Guarding against "the demise of the Archive" satisfies the obligation to protect both the cultural heritage of humanity (provided it can be stored or represented in such an archive),[81] and

[78]Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System (OAIS): Recommended Practice*, 2nd ed., CCSDS 650.0-M-2 (Washington, DC, June 2012), accessed March 6, 2021, `https://public.ccsds.org/Pubs/650x0m2.pdf`, recognized as international standard ISO 14721:2012. Like any reference model, this one sets out what functions compliant systems must have, without specifying how those functions are to be implemented.

[79]" . . . it would be unwise to consider the problem from a solely technical standpoint. There are also organizational, legal, industrial, scientific and cultural issues to be considered. To ignore the problems raised by preserving information in digital forms would lead inevitably to the loss of this information." Consultative Committee for Space Data Systems, §1.3. "An archive that superbly guarantees the integrity of its records will not be useful if the agencies sending records to the archive have been sloppy about any aspect of stewardship of the records in their custody." National Research Council [USA], *Building an Electronic Records Archive*, 69.

[80]Consultative Committee for Space Data Systems, *Reference Model*, §3.1. Other obligations include acquiring "sufficient control of the information provided to the level needed to ensure Long Term Preservation" and providing traceability "to the original submitted Data Objects with evidence supporting its Authenticity." Capitalized terms are defined within the standard. Of particular note is the definition of Data Object as "[e]ither a Physical Object or a Digital Object." Consultative Committee for Space Data Systems, §1.7.2.

[81]Cultural Property Convention, Art. 1–4; AP I, Art. 53.

the obligation to protect the rights of persons by keeping relevant civil records—regardless of the media on which they are recorded—secure from both accidental and intentional harm.[82]

Such an archive is still vulnerable to damage arising from both benign operational mistakes and intentional disruption caused by flouting the laws or regulations governing the archive. Even so, good faith on the part of the organization in following the guidance given by this reference will be sufficient to meet a target state's obligation to protect archival records from damage during times of armed conflict. Since this reference model has broad international support from both government agencies and professional archivists, this model establishes the minimal functional requirement for satisfying this obligation. A state cannot claim to be uninformed about how to discharge this responsibility. Further, as noted in Chapter 5, states party to ICESCR may ask for assistance during peacetime to put these rights-protecting measures in place.[83]

6.6 *Tallinn 2.0* and data objects

Tallinn 2.0 acknowledges that that international law does require protecting certain data objects: those required to provide and manage medical services, including patient records;[84] records and other data required to fulfil obligations to persons detained during an armed conflict;[85] and perhaps significant cultural property stored in digital form.[86] The expert committee did

[82] AP I, Art. 48, under the interpretation that civilians enjoy, as the title of Part IV, Section I reads, "general protection against effects of hostilities." The ICRC notes that "social security data, tax records, bank accounts, companies' client files or election lists or records" in physical form have protection under this general rule without being explicitly identified in the treaties of international humanitarian law. International Committee of the Red Cross (ICRC), "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts," in *32nd International Conference of the Red Cross and Red Crescent*, doc. 32IC/15/11, report (Geneva, CH: International Committee of the Red Cross, December 8–10, 2015), 43, accessed March 6, 2021, `https://rcrcconference.org/app//uploads/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf`; *cf.* *Tallinn 2.0*, Rule 100, comment 7.

[83] ICESCR, Art. 2(1).

[84] *Tallinn 2.0*, Rule 132, comment 3.

[85] *Tallinn 2.0*, Rule 135.

[86] *Tallinn 2.0*, Rule 142, comments 4–6.

not, however, agree on what cultural property is significant when it represented digitally. Some held that because data objects are intangible (even though the media on which they are stored is tangible), they do not meet the description of *cultural objects* in AP I.[87] Others countered that intellectual property is intangible, and yet still has protection as a kind of cultural object, particularly if it exists only in digital form—things like "musical scores, digital films, . . . and scientific data."[88]

The same experts that presented a case for considering digitized data objects as cultural property include "documents pertaining to e-government" among the examples of cultural data objects,[89] and this position is one that is more readily defended. E-government initiatives typically include (among other things) the abilities to register births and deaths through online forms, and to request authenticated extracts from those registries.[90] Thus birth registrations in these e-government systems begin as digital records—intangible as entities, but with a representation on some physical medium. If they are treated as intangible, and thus not eligible for protection as cultural objects, then there is no requirement to make an effort to preserve these records. However, there is an international mandate to record births and a recog-

[87] *Tallinn 2.0*, Rule 142, comment 4.

[88] *Tallinn 2.0*, Rule 142, comment 5. The importance of preserving scientific data was highlighted during the presentation of the first image of a black hole on April 10, 2019, when it was revealed that the data gathered for the project "was too much to be sent across the Internet. Instead, the data was stored on hundreds of hard drives that were flown to . . . central processing centres in Boston, US, and Bonn, Germany, to assemble the information." Pallab Ghosh, "First Ever Black Hole Image Released," *BBC News*, April 10, 2019, accessed April 10, 2019, `https://www.bbc.com/news/science-environment-47873592`. The only way to make this data available to researchers was through a physical transfer of duplicate media, not through a digital network. Other large data-gathering scientific research projects have the same constraint, where distributing the digital records requires distributing the storage media as well.

[89] *Tallinn 2.0*, Rule 142, comment 5.

[90] The province of Ontario has announced its intention to issue digital identity documents, including birth certificates, health insurance certificates, and drivers' licences. Ontario, "Ontario Onwards: Action Plan," November 30, 2020, accessed March 18, 2021, `https://www.ontario.ca/page/ontario-onwards-action-plan#section-3`. If the full information content of those records is not stored on personal smartphones, but mediated by a secure digital identifier associated with the records in the issuer's database, persons may not have physical copies of these documents to compare against the official government record.

nized need to safeguard those records in order to protect the rights of children. Both ICCPR and the Convention on the Rights of the Child explicitly state that every "child shall be registered immediately after birth and shall have . . . a name."[91] Registration does not confer a nationality upon the child, but it does provide documentation that will help determine the child's nationality, and satisfy the right of a child to a name and an identity—the minimal acknowledgement of personhood. States party to these agreements, then, have an obligation to register births, regardless of nationality, in their territory, and to preserve those records in order to preserve the relevant rights ascribed to those persons.[92] Extending this to all vital records is a small step; adding property records is then another step for the protection of not just children, but all persons. Again, the standard framework developed by international experts in archiving provides a strategy for implementing this kind of recording and preservation. There is, then, no principled reason to not provide, preserve, and protect this minimal archive.

Moreover, the minority opinion expressed by the international group of experts in *Tallinn 2.0*'s commentary on Rule 100 ("Civilian objects are all objects that are not military objectives. . . . ") better accords with the ICRC's opinion that these kinds of records, among others

> such as social security data, tax records, bank accounts, companies' client files or election lists or records [are] already protected. . . . Deleting or tampering with such data could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects. The conclusion that this type of operation would not be prohibited by IHL [international humanitarian law] in today's ever more cyber-reliant world—either because deleting or tampering with such data would not constitute an attack in the sense of IHL or because such data would not be seen as an object that would bring into operation the prohibi-

[91] ICCPR, Art. 24(2); Rights of the Child, Art. 7(1).

[92] All 29 member states of NATO are party to the former; only the USA is not a state party to the latter (though it is a signatory). United Nations Human Rights Committee, "Status of Ratification Interactive Dashboard," April 15, 2019, accessed April 16, 2019, `http://indicators.ohchr.org`. Thus, as far as NATO members are concerned, creating and preserving birth records is settled international law, regardless of the medium on which they are recorded.

> tion of attacks on civilian objects—seems difficult to reconcile with the object and purpose of this body of norms.[93]

The ICRC more recently put a finer point on this: "Put simply, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them."[94]

The *Tallinn Manual*'s recognition that digital representations of some intellectual property has protection as cultural property,[95] its acknowledgement of the ICRC's concern,[96] and its admission that mental suffering as a result of acts intended to spread terror—as the destruction of identity documents did in the Kosovo conflict—is a harm that parties to an armed conflict must avoid[97] all support the conclusion that a cyberattack targeting certain civil and personal records can "result[] in other consequences that would qualify the cyber operation in question as an attack."[98] The minority position that some civilian data "is 'essential' to the well-being of the civilian population is encompassed in the notion of civilian objects and protected as such"[99] has stronger support from international humanitarian law and the *Tallinn Manual*'s own interpretation of it than is presented in Rule 100. The phrasing in the *Tallinn Manual* can justifiably be made stronger, clearly indicating that some civil records, regardless of medium, fall under the umbrella of protected civilian objects, and to the extent that they facilitate participation in and enjoyment of persons' cultural heritage, are arguably cultural objects as well.

---

[93] International Committee of the Red Cross (ICRC), "Challenges of Contemporary Armed Conflict (2015)," 43.

[94] International Committee of the Red Cross (ICRC), "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts," in *33rd International Conference of the Red Cross and Red Crescent*, doc. 33IC/19/9.7, report (Geneva, CH: International Committee of the Red Cross, December 9–13, 2019), 28, accessed November 28, 2020, `https://shop.icrc.org/download/ebook?sku=4427/002-ebook` (hereafter cited as Challenges of Contemporary Armed Conflict (2019)).

[95] *Tallinn 2.0*, Rule 142, comment 5.

[96] *Tallinn 2.0*, Rule 100, comment 7, n1058.

[97] *Tallinn 2.0*, Rule 92, comment 8.

[98] *Tallinn 2.0*, Rule 100, comment 6.

[99] *Tallinn 2.0*, Rule 100, comment 7.

6.7 Digital objects and data centres

Digital objects take up very little physical space. The Internet Archive, better known as the Wayback Machine, contains roughly 15 petabytes of data.[100] This is the equivalent of 15 quadrillion typed characters, or 7.5 trillion letter-sized (or A4) pages of text (about one thousand pages for each person currently living), or 1.5 billion boxes of photocopier paper. It also fits on 1500 10-terabyte disks. These disks, plus associated server hardware, can take up as little as 14 square feet of floor space.[101] The paper equivalent fills a few hundred largish buildings: roughly 15,000 floors of 10,000 square feet each. Microform storage reduces this substantially, but still takes at least 50 floors of this size, or one very large office tower, to store.

The compactness of a digital archive means that a physical strike on the building containing that archive (and any facilities containing backups) only has to be small but precise. A small, precise physical attack meets the proportionality criterion of the laws of armed conflict—provided that either the archive itself or the building housing the archive is a legitimate military objective. However, a building or object is only a legitimate military target in armed conflict if it serves (and not merely if it potentially can serve) a military purpose, and if its destruction "in the circumstances ruling at the time, offers a definite military advantage."[102] A data centre that houses information used for military purposes is a legitimate target; one that does not is not.

[100] Kalev Leetaru, "Why Are We So Afraid of Petabytes?," *Forbes*, January 17, 2017, accessed May 1, 2019, `https://www.forbes.com/sites/kalevleetaru/2017/01/17/why-are-we-so-afraid-of-petabytes/#609365765875`.

[101] One manufacturer has equipment that stores this much data in the space provided by two standard server racks. Aberdeen, *Petarack*, Product specification sheet. 2018, accessed May 1, 2019, `https://www.aberdeeninc.com/wwwinc/pdf/Petarack-One-Sheet.pdf`. A standard server rack is 60 cm (23.6 inches) wide, 105 cm (41.34 inches) deep, and 200 cm (78.74 inches) tall; the floor space is a little less than 7 square feet per rack.

[102] AP I, Art. 52(2). Notably, the USA has not ratified, and thus is not a state party to, AP I. Moreover, while AP I limits what counts as a military objective, American military doctrine expands it to include any object that makes an "effective contribution to the war-fighting or war-sustaining capability of an opposing force" (Department of Defense [USA], *Department of Defense Law of War Manual* (December 13, 2016), ¶5.6.6.2, accessed May 1, 2019, `https://www.hsdl.org/?view&did=797480`), regardless of whether it is being used for military purposes in the current conflict. Shue, "Laws of War," 527. This is taken up further in *Tallinn 2.0*, Rule 100, comments 18, 19.

Vital records and civil property records do not, by themselves, serve a military purpose. These records are essential for adjudicating rights claims during and between times of armed conflict, but those are not military functions. There is societal value in preserving them, and I have shown that there are good reasons to hold that states have an obligation to take steps to preserve them from damage. One step is to store purely civil records in a physically separated and identifiable repository. The complete centralization of all of a state's records in a single facility (and a single backup facility) prevents states from satisfying their obligations under international law because it houses them with records that serve a military purpose.[103] This leaves civil records unprotected, because the facility is a lawful target under the laws of armed conflict. Civil records can only be protected from lawful attack by storing them in a data centre that serves only civilian functions, and cannot be intentionally misidentified as one that serves a military function.[104]

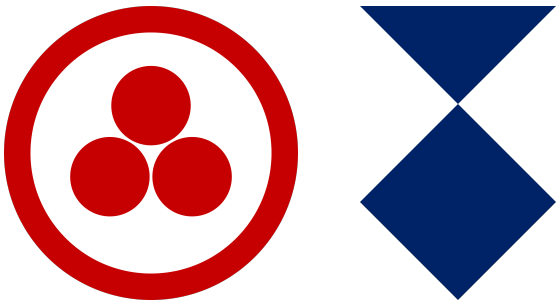
In 2017 Luxembourg and Estonia created a novel solution to the problems of protecting civilian data and guaranteeing its isolation from military data. The two states signed an agreement permitting Estonia to set up a government data centre in Luxembourg with full diplomatic protection, "effectively creating a corner of Estonian sovereign territory in cyberspace, via a data center in Luxembourg."[105] (A separate agreement was necessary because existing diplomatic and consular law does not have provisions guaranteeing the inviolability of data and infrastructure outside the walls of the official embassy.) The virtual data embassy facilitates the continuity of government services should Estonia be unable to provide them from within its borders. Since most of Estonia's civil records, including the official record of government legislation,[106] exist only in digital form, this kind of redundancy is the only way to recover from a crippling cyberattack quickly. The agreement between the two countries also means that an attack on Estonia's data

[103] A *copy* of the civil records can be stored there as long as there is a copy in a separate, purely civilian, repository.

[104] This is no guarantee against their destruction as collateral damage in a strike against a legitimate military objective, but it makes intentional targeting of these records and facilities a violation of international law.

[105] Microsoft Corporation, "Diplomatic Immunity for Data: Estonia Creates a Virtual Embassy," *Microsoft EU Policy Blog*, December 14, 2017, accessed March 7, 2021, `https://blogs.microsoft.com/eupolicy/2017/12/14/diplomatic-immunity-data-estonia-creates-virtual-embassy/`.

[106] Microsoft Corporation.



(a) (b)

Figure 6.1: Symbols marking protected cultural sites. (a) The Roerich Pact banner of peace. (b) The Cultural Property Convention blue shield. Both identify civilian sites of cultural significance that are to be protected from attack. (All images are in the public domain.)

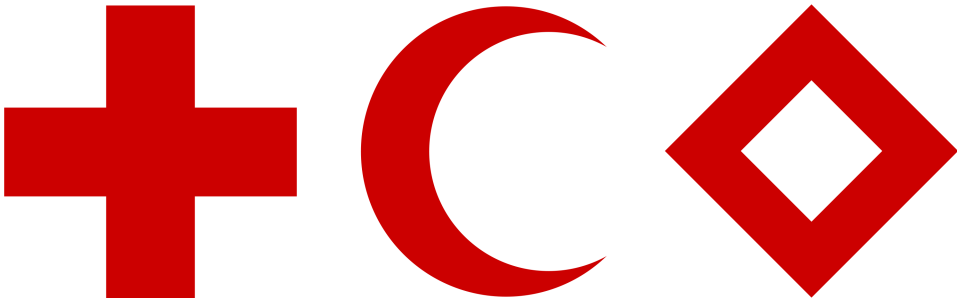
embassy likely also violates Luxembourg's sovereignty,[107] so this arrangement could serve as a foundation for groups of states to be mutual protectors of their civil records, following the model of mutual defence clauses in military alliance treaties.

Of course, the problem of identifying these civilian data centres as protected objects remains. The Cultural Property Convention sets out a distinctive marking that can be used: the blue shield described within the Cultural Property Convention as "a shield consisting of a royal-blue square, one of the angles which forms the point of the shield, and of a royal-blue triangle above the square, the space on either side being taken up by a white triangle."[108] This replaces the "banner of peace" consisting of a "red circle with a triple red sphere in the circle on a white background"[109] specified in the 1935 Roerich Pact for its states parties who have not acceded to the Cultural Property Convention. Both symbols are illustrated in Figure 6.1. These symbols function in the same way that a red cross, crescent, or diamond (Figure 6.2)

[107] *Tallinn 2.0*, Rule 4, comment 19.

[108] Cultural Property Convention, Art. 16(1).

[109] Pan-American Union, Treaty on the Protection of Artistic and Scientific Institutions and Historic Monuments (Roerich Pact), Washington, 15 April 1935, April 15, 1935, Art. 3, accessed January 3, 2020, `https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/EE57F295093E44A4C12563CD002D6A3F/FULLTEXT/IHL-44-EN.pdf` (hereafter cited as Roerich Pact).



(a) (b) (c)

Figure 6.2: Symbols marking protected sites providing humanitarian aid. (a) Red cross. (b) Red crescent. (c) The third protocol emblem, often referred to as the red crystal. The uses of the red cross and red crescent as protective emblems are set out in Articles 38–43 of GC I. The third protocol emblem is described in Article 2 of AP III. (All images are in the public domain.)

does to identify facilities providing humanitarian aid.[110] The banner of peace or blue shield declare that the marked facilities have protection equivalent to that afforded humanitarian aid sites because of their value to humanity.

The blue shield (or equivalent) emblem only asserts protected status when it can be clearly seen by the attacking party. Consequently, this method of marking objects and disclosing locations of protected buildings is fallible. There is plausible deniability about not seeing the markers or otherwise recognizing the building as a protected object, particularly if weaponry is not equipped for visual reconnaissance.

There are two particularly striking examples of misidentifying protected facilities. NATO's (presumably) accidental bombing of the Chinese embassy in Belgrade, Yugoslavia—a protected building in the context the Kosovo conflict—on May 7, 1999, illustrates how easily a protected building and civilians can be harmed through human error. The bombs were intended to destroy the headquarters of a Yugoslavian agency serving their armed forces—a building located about 350 metres away from the embassy.[111] They

[110] GC I, Art. 38, 39, 42; AP III, Art. 2.

[111] Kevin Ponniah and Lazara Marinković, "The Night the US Bombed a Chinese Embassy," *BBC News*, May 7, 2019, accessed May 7, 2019, `https://www.bbc.com/news/world-europe-48134881`.

(a) (b) (c)

Figure 6.3: Symbols marking other protected sites. (a) Oblique red band, described in GC IV, Annex I, Article 6, used to identify civilian hospitals and safety zones established under Article 14 of that Convention. (b) Blue equilateral triangle on an orange field, identifying civil defence facilities and personnel as set out in Article 66 of AP I. (c) Three orange circles, used to mark "works or installations containing dangerous forces," the release of which "may cause . . . severe losses among the civilian population," as described in Article 56 of AP I. Symbols (b) and (c) are shown only for completeness. (All images are in the public domain.)

were programmed with coordinates extrapolated from an outdated map, and there was no record of the Chinese embassy's location in the "intelligence and military databases used to cross-check targets."[112] The Chinese government viewed this grave operational error as a violation of international law, and the American government eventually made compensatory payments to China and the victims' families for the harm done.[113] The second took place on October 3, 2015 in northeastern Afghanistan. The crew of an American AC-130U gunship aircraft destroyed a trauma centre operated in Kunduz by Médecins Sans Frontières (MSF). The hospital was registered on the no-strike list for the area, but through a tragedy of errors fuelled by fatigue, equipment failure, incomplete information, and a cascading lack of situational awareness, it was mistaken for the intended target: a suspected Taliban-controlled site about 450 metres away.[114] While the hospital did not have any markings described in GC I (Figure 6.2) or GC IV (Figure 6.3(a)) identi-

[112] Ponniah and Marinković.

[113] Ponniah and Marinković.

[114] United States Central Command, *Investigation Report of the Airstrike on the Médecins Sans Frontières / Doctors Without Borders Trauma Center in Kunduz, Afghanistan on 3 October 2015*, in-

fying it as a protected site,[115] it had been reported that a large MSF flag was clearly displayed on the roof of the building.[116] Further, there was no positive identification of active combatants at the hospital by anyone involved, so under the principle of distinction the building was to be presumed to be a civilian facility.[117] The investigation found clear violations of mission rules of engagement and the laws of armed conflict[118] because the hospital had been attacked without evidence of it being used for a military purpose. Again, the American government made compensatory payments to the families of the victims and contributed money toward the rebuilding of the hospital.[119]

In a similar vein, cyberattacks have no means to spot markings around protected buildings. They only recognize data stored on some kind of digital medium. The type of medium may be discoverable by the attacking software, but there is no convention within a computing device's operating system to mark particular media as containing only civilian data objects. Even if there were, malware can readily ignore them, in violation of the principle of distinction.[120] *Tallinn 2.0* proposes this kind of data marking, at least for

vestigation report and summary (November 25, 2015), summary, [1–2], accessed September 5, 2020, `https://web.archive.org/web/20190331041350/https://info.publicintelligence.net/CENTCOM-KunduzHospitalAttack.pdf`.

[115] United States Central Command, summary, [3].

[116] Joseph Goldstein, "Doctors Without Borders Says Clues Point to 'Illegal' U.S. Strike on Afghan Hospital," *New York Times*, November 5, 2015, accessed September 5, 2020, `https://www.nytimes.com/2015/11/06/world/asia/doctors-without-borders-seeks-explanation-for-kunduz-hospital-attack.html`. The post-incident report noted that there were actually two flags on the roof of the main building. United States Central Command, 47. It is not clear whether MSF had authorization from the government of Afghanistan to use official Geneva Convention markings. United States Central Command, 47n255, referring to GC IV, Art. 18, ¶3. Using the MSF flags in lieu of officially recognized symbols would have been a best-effort attempt to provide a visual signal that it was a protected facility.

[117] United States Central Command, 75–6.

[118] United States Central Command, summary, [3].

[119] United States Central Command, summary, [5].

[120] Ignoring markings and directives already happens. Web sites and the programs that search them use an informal protocol called the *Robots Exclusion Protocol*. If a web server contains a file named `robots.txt` in its top-level directory, any automated tools—software robots—looking at the entire contents of that server are expected to read this file to determine where they are not "allowed" to look. This is about as effective as telling a cat that it is not allowed on the dining room table. It will go there anyway. The authoritative web site on this protocol points this out, adding "[e]specially malware robots that scan the web for security vulnerabilities, and email address harvesters used by spammers will

information concerning medical services:

> All feasible measures shall be taken to ensure that computers, computer networks, and data that form an integral part of the operations or administration of medical units or transports are clearly identified through appropriate means, including electronic markings. Failure to so identify them does not deprive them of their protected status.[121]

The party marking the data as protected is expected to notify the other party in the conflict what the marks are, and in turn expects the other party to verify that those files, devices, or systems do not and are not likely to serve a military purpose.[122] As fragile as such a protocol is, there is no better scheme currently to be had, and it is no more fragile than other protocols identifying civilian and humanitarian facilities. The onus is still on the attacking party to determine the protected status of data objects, regardless of whether they are marked or not. This, though, has another risk: the nature of the protected data has to be verifiable, so if the data is encrypted, the relevant encryption keys have to be exchanged, and so any personal information protected by privacy laws may be exposed to a party that does not provide equivalent protection. States may have to place modest limits on some of their residents' privacy rights in order to preserve the records that support other civil rights.

6.8 Data protection in just war

As civil records move from paper or microform to digital media they become susceptible to alteration and vulnerable to accidental or intentional destruction. But these records are essential to support granting rights and privileges of various sorts. Defending the rights of persons to certain things requires protecting these records, and this requires at least two distinct measures: secure replica repositories, and identifying these repositories as protected objects of national and cultural significance in both physical and cyber realms. I have already shown that both of these measures are currently practicable if

pay no attention." robotstxt.org, "About */robots.txt*," 2007, accessed May 12, 2019, `http://www.robotstxt.org/robotstxt.html`.

[121] *Tallinn 2.0*, Rule 133.

[122] *Tallinn 2.0*, Rule 133, comment 5.

the international community has the will to implement them. Now I turn to how this kind of protection serves humanitarian purposes in just-war terms.

Violations of *jus in bello* obligations

Vital statistics records are among the data objects bearing national or cultural significance. However, some of these records are evidence of more than just citizenship. They are also a record of a person's mere existence.[123] One of the primary purposes of international humanitarian law is to set out "the duty to prevent genocide,"[124] and a genocide is easier to conceal if there is no record of the victims. The ethnic cleansing actions of the 1998–99 civil war in Kosovo illustrates the importance of having a verifiable identity. This conflict included a process now called *identity cleansing*:[125] seizing and destroying identity documents from persons, archives, and registries. Property records were also destroyed. Not having these documents kept people from having homes, jobs, and access to services.[126] But for those who died without a record of identity, it is as if they never existed. Their nameless bodies might be accounted for in a death toll, but without identity documents it is impossible to say with certainty that they were victims of a genocide.

Protecting identity records preserves evidence of persons' existence. In times of armed conflict a target state taking steps to protect these records will hinder an aggressor state's ability to pursue genocide as a means of war—one that is non-discriminatory and evil in itself, and so prohibited under the rules of *jus in bello*. Conversely, an aggressor state's intentional destruction of these records may foreshadow an ethnic or cultural purge if the target state's territory is overrun.

---

[123] United Nations High Commissioner for Refugees (UNHCR), *Birth Registration*, Child Protection Issue Brief, Geneva, CH, August 2013, 2, accessed April 11, 2019, `https://www.refworld.org/docid/523fe9214.html`.

[124] *Tallinn 2.0*, Rule 6, comment 6.

[125] *U.S. Department of State Country Report on Human Rights Practices 2002 — Yugoslavia, Federal Republic of*, United States Department of State, March 31, 2003, "Kosovo," §2d, accessed March 28, 2018, `http://www.refworld.org/docid/3e918c46c.html`.

[126] "Because cultural expression and institutions express identity so concretely it becomes necessary to extinguish the group's cultural expression and expunge from dispute territories any evidence of the group." Rebecca Knuth, *Libricide: The Regime-Sponsored Destruction of Books and Libraries in the Twentieth Century* (Westport, CT: Greenwood Publishing Group, 2003), 64.

The protection of identity records is also justified under the ICJ's interpretation of international humanitarian law in its 1996 *Nuclear Weapons Advisory Opinion*, not because of a particular means of war, but because one of the "cardinal principles . . . of humanitarian law . . . is aimed at the protection of the civilian population and civilian objects."[127] Civil records are civilian objects, and while a state may use them to determine who may be obliged to provide military service, there is yet no justification that they serve any active military purpose. Thus the principle of discrimination of *jus in bello* also applies to these data objects.

Experience has shown that where there is no will to honour the rules of *jus in bello*, it will not likely be followed. States, therefore, must be permitted to counter attempts by aggressor states to harm or destroy civil records, regardless of how or where those records are stored. To this end, then, in defence of its citizens' rights and in alignment with the right to defend or repel an attack against other civilian targets, a proportionate forceful response, either cyber or conventional, may be justified to end an attack targeting those records. A diplomatic claim demanding reparations may facilitate reconstructing those records, to whatever extent is possible, is justified afterward. Even so, the best (and probably least expensive) defence against this kind of destruction is to have multiple digital copies distributed among archival sites. Moreover, since these records do not serve military purposes, this may include having a copy hosted securely in a third-party state without violating the principle of neutrality, as Estonia and Luxembourg have agreed to do.

Facilitating *jus post bellum*

If, as Henry Shue suggests, "[t]he purpose of the laws [of war] is to minimize the rights violated and the evils committed, . . . to constrain the 'shit' when the 'shit' happens,"[128] then it seems just to address those violations and restore, as far as possible without sowing the seeds for another conflict,[129] the rights of civilians in a deliberate but urgent fashion *post bellum*. Just as safeguarding civil records from damage can serve as an evidential hedge against

[127] *Nuclear Weapons Advisory Opinion*, ¶78.

[128] Shue, "Laws of War," 515–16.

[129] Brian D. Orend, "Justice after War," *Ethics & International Affairs* 16, no. 1 (March 2002): 43, accessed October 25, 2015, https://doi.org/10.1111/j.1747-7093.2002.tb00374.x.

a genocide during a war, they can also help in reconstructing a civil society after one.

Again, the Kosovo conflict is illustrative, both with respect to the difficulty of the task when records have been destroyed, and to the importance of doing this task well. The forcible stripping of identity records from those fleeing the conflict was intended to ensure that citizens of Albanian origin had no "right to return to their homes."[130] A just restoration after the conflict would require granting these persons access to their former residences.[131] However, many Albanians had already been deprived of their residences before the 1998–99 conflict after the Serb-dominated government of the Federal Republic of Yugoslavia revoked Kosovo's autonomy and instituted pro-Serbian employment and housing policies in 1989.[132] Moreover, some members of the Serbian community also suffered displacement.[133] The competing claims to property due to missing records, altered records, and unrecorded transfers,[134] coupled with fear of violence and lack of will to enforce judgements,[135] have caused lengthy delays in restoring persons to

[130] *Milutinović* indictment, ¶31.

[131] "The safe and dignified return of DPs [displaced persons] to their homes is one of the fundamental rights contributing to a stable multi-ethnic society in Kosovo." Organization for Security and Co-operation in Europe (OSCE) Mission in Kosovo, *An Assessment of the Voluntary Returns Process in Kosovo*, Returns and repatriation report (Organization for Security and Co-operation in Europe, October 2012), 5, accessed May 12, 2019, https://www.osce.org/kosovo/96805?download=true.

[132] Organization for Security and Co-operation in Europe (OSCE) Mission in Kosovo, *Challenges in the Resolution of Conflict-Related Property Claims in Kosovo*, Returns and repatriation report (Organization for Security and Co-operation in Europe, June 2011), 4n8, accessed May 12, 2019, https://www.osce.org/kosovo/80435?download=true; Serbeze Haxhiaj and Filip Rudic, "Lost Property: Kosovo's Missing Records Prolong Post-War Legal Battles," *Balkan Insight*, April 3, 2019, accessed May 12, 2019, https://balkaninsight.com/2019/04/03/lost-property-kosovos-missing-records-prolong-post-war-legal-battles/.

[133] Organization for Security and Co-operation in Europe (OSCE) Mission in Kosovo, *Challenges in Resolution*, 7–8.

[134] Scott Leckie, "Resolving Kosovo's Housing Crisis: Challenges for the UN Housing and Property Directorate," *Forced Migration Review* 7 (April 2000): 13–14, accessed May 15, 2019, https://www.fmreview.org/sites/fmr/files/FMRdownloads/en/land-and-property-issues/leckie.pdf; Haxhiaj and Rudic, "Lost Property."

[135] Organization for Security and Co-operation in Europe (OSCE) Mission in Kosovo, *An Assessment of the Voluntary Returns Process in Kosovo*, Returns and repatriation report (Organization for Security and Co-operation in Europe, October 2014), 14, accessed May 16, 2019, https://www.osce.org/kosovo/129321?download=true.

their homes, and even those who have returned home do not always feel secure there.[136] This aspect of *jus post bellum* will not be attained in Kosovo, or anywhere else, until accurate identity and property records are established, accepted as authoritative, and enforced.

6.9 Conclusion

The advent of cyberwarfare did not create the problem of safeguarding civil records. It exposes and exacerbates it. In this chapter I have argued that international humanitarian law requires recording and preserving birth records, and that preserving human rights *post bellum*—or indeed after any disaster—requires recording and preserving property and other civil records. Further, I have established that the reconstruction of a civil society after an armed conflict is facilitated by preserving some aspects of cultural heritage including unique and significant artefacts that represent human creativity and achievement. I have shown that there are archival best practices that will allow states to satisfy these obligations regardless of their choice of technology.

I have also shown that the space efficiency provided by digital archives makes them particularly vulnerable to physical harm. There are international conventions for designating and identifying facilities as serving strictly civilian purposes, and these kinds of records and cultural objects are entitled to the protection of the *jus in bello* principle of distinction. A digital, network-accessible marking should be agreed upon for identifying systems that store and process these protected digital objects, and all parties to a conflict should respect those markings, though it is a very easy thing to ignore when creating software to disable a military objective. Nonetheless, the protection of digital archives can still be satisfied under the broad terms of existing international humanitarian law; it only needs explicit interpretation for protecting digital objects stored in strictly civilian data centres.

[136] Organization for Security and Co-operation in Europe (OSCE) Mission in Kosovo, 16–17.

Chapter 7

Continuing the project

7.1 Summary of findings

This project has shown that even though the means and methods of cyberwarfare are novel, there is no relevant significant difference between them and existing conventional means and methods of warfare. The Martens Clause of HC II (1899),[1] which is reiterated in the ICJ in its *Nuclear Weapons Advisory Opinion*,[2] subjects all means and methods of warfare to the international laws of armed conflict. The challenge is interpreting those laws in such a way that treats novel means of warfare in the same spirit and language as conventional ones. In Chapter 2 I have set out a robust but open-textured description of a cyberattack, then addressed each of Randall Dipert's important questions concerning the justification of cyberattacks and responses using existing international law, concepts from just-war theory, and two real-world cyberattacks, demonstrating that the challenge Dipert poses can be met.

The *Tallinn Manual*, developed in the aftermath of a crippling cyberattack against Estonia, provides an interpretation of existing international law in the context of aggressive cyberoperations. Chapter 3 argues that since the

[1] "Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience." HC II (1899), preamble.

[2] *Nuclear Weapons Advisory Opinion*, ¶87.

Internet's operators rely on laws and norms in order to provide the service, and since the Internet has been a vector of attack against state interests, an analysis of international law along the lines of the *Tallinn Manual* is justified to establish states' rights and responsibilities with respect to network and data operations. It also shows that the *Tallinn Manual* stands in the tradition of war manuals that distil the laws of armed conflict into a collection of reliable, though imperfect, rules, and that the process and persons that produced the *Tallinn Manual* give it credibility and authority. Chapter 4 gets more theoretical and technical, showing how the *Tallinn Manual* comports with the norms of just-war theory, concluding that the *Tallinn Manual* not only upholds those norms to the extent that current international law does, but also goes further by giving consideration to matters of just cause and human rights. This justifies accepting the *Tallinn Manual* as a starting point for wrestling with the interpretation of international law with respect to cyberwar.

The following chapter introduces concepts that apply the *Tallinn Manual*'s guidance to assess the severity of a cyberattack and bound the permissible responses to an aggressive cyberoperation. The international laws of armed conflict, and in particular the UN Charter, permit states to defend themselves against armed attacks and lesser uses of force by other states. Under the *jus in bello* obligation of proportionality, these defensive responses are limited to what is justifiable to end the threat or attack based on the information available at the time. In determining whether an act of aggression committed by cyber means has reached the level of a conventional armed attack, the *Tallinn Manual*'s scale-and-effects doctrine is directly applicable when physical harm is readily apparent, but its applicability is limited when the harm is not perceptible or has not yet occurred. I show that the inability to assess unperceived harm is common to both conventional and cyber means of warfare. In cases of imperceptible harm, the question of whether a cyberattack can be considered a moderate use of force or a flagrant attack equivalent to a conventional armed attack depends in part on epistemological states—what is (or can be) known about the intended and potential effects of the aggressive operation. It does not depend on the means by which the action is carried out. Further, I demonstrate that the effects of both conventional and cyber attacks can affect the enjoyment of human rights acknowledged under various treaties. Those impacts can be considered part of the effects

of an attack, and so factor into the determination of whether a cyberattack crosses the boundary from moderate to flagrant.

While the scale-and-effects criteria are useful, the *Tallinn Manual*'s related assessment criteria of causal directness and temporal immediacy do not provide consistent guidance when effects take a long time to develop. Chapter 5 introduces an extended temporal model of attack and effects to demonstrate that the maximum justifiable response to a use of force depends on when the target state becomes aware of any harm that may arise from an aggressive action against it—an action that may have been proceeding undetected for a long period of time and may not have produced more than an inconvenience to the target state. A state's ability to recognize and neutralize potential harm limits the justification for making a nocuous or a moderate response, even though the origin of the attack has been determined and there is a short, direct causal chain between the start of the attack and the recognition that there is unrealized harm to avert.

The novelty of cyberwarfare does highlight how cultural and data objects are vulnerable to destruction during times of conflict. While some cultural objects deemed to be of value to humanity in general are protected from intentional targeting under international conventions and the laws of armed conflict, the data objects—records of birth, residency, and property ownership—needed to satisfy human rights obligations and sustain a civil society are also of sufficient value to humanity in general that they, too, merit being designated as protected objects. This protection must extend to the facilities housing these records. Chapter 6 makes this argument on the basis of human rights declarations, international humanitarian law, and international standards of archival practice. Protecting these records from harm involves both proactive measures *ante bellum* (or, perhaps more cynically, *inter bella*) and respect for such facilities *in bello*, so there is a possibility of a sustainable minimally just society *post bellum*. This goes beyond the scope of the *Tallinn Manual*, but not beyond the international conventions already in place with respect to protecting both human rights and cultural objects. This protection requires international agreement on protocols specific to data in cyberobjects, but it does not require any new conventions. However, effective protection, just as the protection of civilians during times of armed conflict, requires a political commitment among belligerent parties in a conflict to honour those conventions and protocols.

7.2 Directions for future work

My short exploration of aggressive cyberoperations in the context of international armed conflict necessarily leaves follow-on questions untouched. This is a small selection, each of which could be an extended discussion on its own.

Separating *data* from *cyber*

Two interpretations; two priorities

The *Tallinn Manual* recognizes a distinction between *data* and *cyber* that can best be summarized this way: not all data is cyber, and not all of cyber is data. It does not claim authority to address matters concerning harm to data except where it is connected with cyberoperations. In contrast, the Shanghai Cooperation Agreement makes a clear separation between the two. The Agreement uses the term *information* in a way that includes *data* as understood in the *Tallinn Manual*, but also incorporates the information content represented by the data, regardless of the medium of storage or transmission. That leaves *cyber* as referring to the use of digital communications and computing technology to store, transfer, and process that information; that is, computer networks form one class of what it calls *information infrastructure*.[3] The significance of this distinction is revealed in the Agreement's definition of *information war*:

> confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, critical and other structures, undermining political, economic and social systems, mass psychologic brainwashing to destabilize society and state, as well as to force the state to taking decisions in the interest of an opposing party[.][4]

Note that *cyberwar* itself is not a primary concern; rather, the greater concern with respect to state sovereignty appears to be maintaining control over information, in all of its breadth, as a critical national interest.

[3] Shanghai Cooperation Agreement, Annex 1.

[4] Shanghai Cooperation Agreement, Annex 1.

One way to understand the different approaches is that the *Tallinn Manual* is recognizing the shift in political thinking from the idea that each state is responsible for maintaining its own sovereignty and is free from the influence of other states with respect to purely internal matters (which largely held until the end of the First World War), to one where states are mutual guarantors of equal sovereignty and protectors of fundamental human rights under an expanding collection of treaty obligations (which finally gained traction at the end of the Second World War). This puts state sovereignty in the service of internationally recognized universal human rights, not in the role of absolute domestic power and distributer of privileges. The Shanghai Cooperation Agreement acknowledges "the important role of information security in the field of ensuring human and civil rights, and fundamental freedoms,"[5] but it also sees "[d]issemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States" as a threat that

> . . . is characterized by the appearance and replication of information in digital (radio and television) and other mass media, on the Internet and other information exchange networks that:
>
> - distorts the perception of the political system, social order, domestic and foreign policy, important political and social processes in the State, spiritual, moral and cultural values of its population . . . [6]

On this account, disseminating information about universal human rights could be seen as disruptive to the interest of states that have no desire to respect or protect them. The protection of the state from the unwanted influence of information (even factual information) coming from outside the state appears to trump the rights of citizens to the freedoms of opinion and of seeking and receiving "information and ideas of all kinds, regardless of frontiers, . . . through any . . . media of his choice."[7] While the Shanghai Cooperation Agreement demonstrates that it is the specific information content of generated, stored, transmitted, processed, or (in the case of software)

[5] Shanghai Cooperation Agreement, preamble.
[6] Shanghai Cooperation Agreement, Annex 2, ¶5.
[7] ICCPR, Art. 19(1), (2).

executed data that is at play in cyberwarfare and information warfare (for example, propaganda and psychological operations), not the uninterpreted data. Cyber infrastructure is just the medium by which the actions are carried out.

Classes of information

The ICRC has articulated a position somewhere in between the ones expressed in the Shanghai Cooperation Agreement and the *Tallinn Manual*. "The ICRC understands 'cyber warfare' as operations against a computer or a computer system through a data stream, when used as means and methods of warfare in the context of an armed conflict, as defined under IHL."[8] A cyberweapon is just one information object contained in the data stream; the cyber infrastructure is the medium that carries the weapon. Stored data is just a frozen data stream until it is accessed or transmitted.[9] The data stream (whether it is stored, being transmitted, or being executed) can contain many kinds of information objects, each serving different purposes.

Classifying data according to the purpose of its information content can help determine whether a cyberattack is moderate or flagrant. Some information is related to critical national interests, whether it be on government systems (for example, civil records and foreign intelligence) or privately-owned systems (for example, banking records, business planning documents, and programs that control a vehicle's speed). Intellectual property may not be of immediate national interest, but it has cultural, personal, or commercial importance for its creators and owners, and those may be critical national interests. If a cyberattack is precisely crafted, like Stuxnet (Chapter 2) and Sunburst (Chapter 3), the target, and thus the intended effects, could eventually be determined. If the intention is to damage particular data, then the character of the relationship of that data to critical national interests will affect the assessment of the attack's severity, and thus the scope of any permissible response to the attack. As discussed in Chapters 5 and 6, damaging

[8] International Committee of the Red Cross (ICRC), "Challenges of Contemporary Armed Conflict (2015)," 39.

[9] The idea of a data stream is a fundamental part of the C++ and other programming languages. The content encoded in that streamed data only becomes accessible and meaningful when that program interprets the data in a purpose-specific way. As far as the computer executing the program is concerned, the data is just a bag of bits.

information that supports a state's sovereignty and ability to satisfy international obligations with respect to human rights and other treaties is a more serious attack than one that, for example, changes the programmed synchronization of traffic lights on a city street in the wee hours of the morning. Having a rubric to map the kind of information harmed by a cyberattack to its severity as a just-cause criterion for a forceful response will supplement the framework I set out in Chapter 5 while avoiding the overreaching claims of sovereignty over information made in the Shanghai Cooperation Agreement. It will also be a step toward the ICRC's goal of understanding "the potential human cost of cyberwarfare."[10]

Human rights in cyberspace

It is incongruous to advocate for protection of some human rights under the international laws of armed conflict while denying that these rights are protected outside times of international armed conflict. The *Tallinn Manual*'s discussion of human rights with respect to personal cyberactivity outside times of armed conflict draws in international instruments setting out human rights and states' obligations such as the UN Charter, the Universal Declaration, ICCPR, and ICESCR. While the *Tallinn Manual* claims that there is agreement that international human rights law does apply to natural persons' activities in cyberspace,[11] it concludes that there is not enough agreement on the details of what those rights entail for anything more than that claim to be accepted as international law. There are two particular sticking points that are attracting attention in contemporary Western society, and they stand at opposite extremes of personal exposure: the freedom from arbitrary state interference with one's privacy[12] and the freedom of expression.[13]

Freedom of expression is a negative right: outside of declared states of public emergency,[14] the only restrictions a state may place on the expression

[10] International Committee of the Red Cross (ICRC), "Challenges of Contemporary Armed Conflict (2015)," 40.

[11] *Tallinn 2.0*, Rules 34, 35.

[12] ICCPR, Art. 17.

[13] ICCPR, Art. 19.

[14] ICCPR, Art. 4.

of "information and ideas of all kinds"[15] are those that protect the rights of others, preserve public order or public health, are needful for national security, or uphold some other local standard of morality (though this last item leaves a lot of room for a state to reshape or impose those standards).[16] The *Tallinn Manual* affirms these restrictions with respect to cyberactivity because of the rights-infringing harms they can produce outside the cyber realm.[17] However, protecting the rights of others sometimes means a reduction in the degree of privacy a person may have online,[18] as long as the state is clear about what the effects of the restrictions are on individual persons.[19]

What does privacy look like in cyberspace? ICCPR asserts the freedom from "arbitrary or unlawful interference with his privacy . . . or correspondence,"[20] so analogies to physical objects again may be useful here. An ordinary email message can be usefully compared to a postcard. The recipient's name and address, the message, and the name of the sender are in plain view. Early Internet email protocols made the same information visible by default. But if the sender puts the postcard in an envelope, only the name and address of the recipient is visible—there is no need to put a return address on the envelope for the mail to be delivered. Further, by putting the postcard in an envelope, both the sender and receiver have an expectation that the message is not subject to inspection by the postal service. Similarly, encapsulating the content of an email in some kind of digital equivalent to an envelope should provide the same assurance to the sender and receiver.

However, all data sent over the Internet is broken up into small chunks called packets, and these contain source and destination information—there is almost always a digital equivalent to a return address on a packet. The content of a packet is interpreted on the destination end, but it can also be examined at other network nodes while it is being transmitted. Some higher-level protocols, such as the streaming video protocols used by services like Netflix, include data in the packet identifying the kind of content carried by the packet, and this is useful for giving priority or preferred routing to certain Internet services. But if a packet can be interpreted to find this kind

[15] ICCPR, Art. 19(2).
[16] ICCPR, Art. 19(3).
[17] *Tallinn 2.0*, Rule 37.
[18] *Tallinn 2.0*, Rule 37, comments 5, 6.
[19] *Tallinn 2.0*, Rule 37, comment 13.
[20] ICCPR, Art. 17(1).

of service-related data, its content can also be sniffed for plain-text words or phrases (for example, *bomb* or *Daesh*) that may trigger further examination of every available packet in the transmission. The need for Internet services to run efficiently can facilitate the routine breach of the expectation of confidentiality. This is, at least in the North American context, a commercial issue, but it is also a rights issue when states take steps to justify inspecting the data content of Internet transmissions (deep packet inspection) for surveillance purposes simply because the service itself requires limited data inspection. What degree of packet inspection becomes an infringement of the ordinary right to privacy?[21] Do financial and medical Internet-based services require positive steps to ensure this right is protected?

Questions also arise around the use of encryption and the conflict with lawful interception of personal data or correspondence. Does the freedom from interference with privacy mean that encryption is permitted and encouraged, placing a technical limit on the ability for states to inspect Internet transmissions, or does it mean that encryption is discouraged and in exchange the government, as protector of the right, will not ordinarily inspect the content of Internet packets, but will take steps to try and punish cybercriminals and others who do? Legal liability has pushed commercial Internet users to the former with respect to data transmission, but personal information stored on data servers in unencrypted form may still be subject to warrantless inspection for legal purposes.

State sovereignty

Election interference

States party to ICCPR are expected to have some kind of electoral process whereby citizens may "take part in the conduct of public affairs, directly or through freely chosen representatives."[22] This obligation requires creating or maintaining some kind of record system to support voters' eligibility claims. Voter lists are the kinds of records that are essential for democratic states to function, but unlike the records set out in Chapter 6, they are not required to safeguard non-derogable human rights or prosecute violations of those rights.

[21] *Tallinn 2.0*, Rule 35, comment 9.

[22] ICCPR, Art. 25(1).

The well-documented vulnerabilities in certain voting machines in current use in the USA[23] leave the tallies open to manipulation,[24] and some voter databases have been accessed (if not modified) by foreign actors.[25] Tampering with voter lists and vote tallies interferes with the state's obligation of "guaranteeing the free expression of the will of the electors,"[26] and is a violation of a state's sovereignty.[27] Further, it raises questions about the legitimacy of any government elected under that interference. If this activity can be attributed to a foreign government, then this disruption of elections meets the invasiveness criterion for just cause,[28] though any civil unrest produced as a result does not meet the directness criterion in a way that can be attributed to the attacking state. Under the framework presented in Chapter 5, this would be no more than a moderate cyberattack, and so a nocuous response would be impermissible. However, diplomacy is unlikely to end the pattern of interference. What moderate measures can a state devise to respond to (and end) attacks on its electoral processes? Does the state's government have an obligation to its citizens to pursue them? Would the current government have a definable interest or obligation toward taking action to secure the next election, particularly if its own legitimacy is in question?

Inciting hatred and violence

Inciting hatred and violence is prohibited under human rights law.[29] States party to ICCPR are obliged to establish a domestic law prohibiting those actions, and any such law must "safeguard individuals from human rights

[23] Joseph Marks and Tonya Riley, "The Cybersecurity 202: U.S. Voting Machines Vulnerable to Hacks in 2020, Researchers Find," *Washington Post*, September 27, 2019, accessed October 6, 2020, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/09/27/the-cybersecurity-202-u-s-voting-machines-vulnerable-to-hacks-in-2020-researchers-find/5d8cf823602ff14beb3da99e/.

[24] Kevin Monahan, Cynthia McFadden, and Didi Martinez, "'Online and Vulnerable': Experts Find Nearly Three Dozen U.S. Voting Machines Connected to Internet," *NBC News*, January 10, 2020, accessed March 8, 2021, https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436.

[25] CBS Chicago, "Illinois Election Chief to Testify at Senate Panel on Russian Hacking."

[26] ICCPR, Art. 25(2).

[27] *Tallinn 2.0*, Rule 4, comment 16; Rule 66, comment 2.

[28] *Tallinn 2.0*, Rule 69, comment 9(d).

[29] "Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law." ICCPR, Art. 20(2).

abuses that are initiated in cyberspace, but may affect their rights offline."[30] When this kind of messaging originates outside a state (for example, from an Eastern European *troll farm*[31] paid to post divisive content to widely-used social media services such as Facebook, Twitter, and YouTube), enforcement of these laws directly against the posting party is not possible. However, the messages are present on servers in the states where these services operate. If a state is party to ICCPR, and those messages are stored on a server in that state, and those messages are aimed at inciting harm within that same state, then the obligation to protect rights violations suggests some sort of action must be taken to remove those messages from view.[32]

A significant problem arises when these Internet services are for-profit commercial operations. Businesses, generally speaking, are not in the business of enforcing laws that fall outside the scope of their operations, so they are not responsible for enforcing laws against external parties on behalf of the state. How should this responsibility to protect rights be shared between the state and the service-providing businesses operating within the state, particularly when the service providers are not creating the offending messages? Is it a business' responsibility to help safeguard the society in which it operates? It seems that since the business depends on at least some elements of a stable and well-functioning society for it to exist at all, it is in the interest of the business to participate alongside the state in this safeguarding activity.[33] What measures can it take to protect itself and society from incitement to hatred and violence that are not themselves violations of other rights?

Economic disruption

As the *Tallinn Manual* notes, there is increasing concern about aggressive cyberoperations targeting civilian commercial and industrial infrastructure to

[30] *Tallinn 2.0*, Rule 35, comment 7.

[31] "A 'troll farm' is an organized operation of many users who may work together in a 'factory' or from different places across a distributed network to generate online traffic aimed at affecting public opinion, and to spread misinformation and disinformation." Mike Snider, "Robert Mueller Investigation: What Is a Russian Troll Farm?," *USA Today*, February 16, 2018, accessed October 7, 2020, `https://www.usatoday.com/story/tech/news/2018/02/16/robert-mueller-investigation-what-russian-troll-farm/346159002/`.

[32] *Tallinn 2.0*, Rule 36, comment 7.

[33] Jordan et al., *With a Clear Conscience: Business Ethics, Decision-Making, and Strategic Thinking*, 250–1.

bring about economic disruption.[34] While there is movement toward these kinds of activities being treated as violations of sovereignty, right now they are, at their most severe, international civil crimes unless a foreign government is demonstrably involved in the operation. In Chapter 4 I discuss economic disruption as a result of sanctions being permitted under current international law, and in Chapter 5 I touch briefly on how economic harm does not typically produce direct physical harm at the scale that a conventional armed attack does. Either kind of disruption may still be a violation of rights.

This problem is magnified when transnational industries rely on infrastructure distributed across multiple states (for example, the automotive industry in Canada, the USA, and Mexico). A cyberattack targeting part manufacturers in Mexico will have a follow-on effect in the other two countries where those parts are used to assemble vehicles. If the goal of the cyberattack is to disrupt the manufacturing sector in the USA, taking Mexico's production offline may be the most effective way to do that. But Mexico then becomes an unwilling third party state in the conflict. If the attack is state-supported, then the attacking state has violated Mexico's sovereignty and neutrality.[35] Such an action would trigger Mexico's obligation to respond in a way that upholds its responsibilities under the relevant treaties and international law. Any consideration of assessing and redressing economic harm caused by cyber means must take into account the fact that states' economies have sectors that are connected to other states' economies. Economic harm will cross borders and oceans, so an attacking state may draw a diplomatic (or stronger) response from states other than the one directly attacked but are nonetheless affected. The fundamental moral and legal principles needed to make sense of economic harm—whether caused by conventional or cyber means—need to be identified, knowing that, just as in the laws of armed conflict, no single one of those principles is likely to be absolute or primary.

Non-state actors

International law, by and large, does not address non-state actors such as private individuals, non-government businesses, and activist or terrorist groups

[34] *Tallinn 2.0*, Rule 4, comment 28.

[35] *Tallinn 2.0*, Rule 150, 151.

regardless of their hierarchy or degree of organization.[36] They are not party to international agreements.[37] The *Tallinn Manual* notes that a harmful cyberoperation launched by a non-state actor might be a breach of the host state's international obligation to "exercise due diligence in ensuring territory and objects over which [states] enjoy sovereignty are not used to harm other States."[38] The target state may be justified in taking countermeasures against the host state if this obligation is not kept.[39] States that do not have the means to exercise this due diligence then become vulnerable to moderate countermeasures—and in extreme situations, perhaps even a nocuous response—as a result of a non-state actor operating against another state without the host state's sanction. While there are documented best practices for safeguarding cyber infrastructure, implementing those best practices takes money and resources smaller states may not have. It seems, then, that countermeasures against a host state must be measured in part by that state's ability to exercise robust, technically sophisticated oversight of its cyber infrastructure. The appropriate response might be to offer technical assistance in providing this oversight[40] rather than inflicting harm in response.

States are gradually adopting the stance that, against current international law, an attack made by a non-state actor can trigger the right of self-defence even without giving the state where the attackers operated a chance to stop the operation.[41] The paradigm example is the series of attacks against the USA by al-Qaeda on September 11, 2001.[42] The government of Afghanistan (to the extent that it had one) may have approved of the attacks, but the state itself was not directly involved. Nonetheless, the American response did in-

[36] *Tallinn 2.0*, Rule 17, comment 2; Rule 33, comment 1.

[37] International organizations are also technically non-state actors, but they are established with state sanction, do not have the rights of states to self-defence, and have obligations to uphold applicable international law and any relevant treaties. *Tallinn 2.0*, 153–7.

[38] *Tallinn 2.0*, Rule 6, comment 1.

[39] *Tallinn 2.0*, Rule 4, comment 4.

[40] *Tallinn 2.0*, Rule 4, comments 31. This assistance can also be offered to states being targeted by a cyberattack. In October 2019 US Cyber Command worked with the Montenegrin government to understand how Russian attacks on its government networks operated. Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020, accessed October 14, 2020, `https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity`.

[41] *Tallinn 2.0*, Rule 71, comment 19.

[42] *Tallinn 2.0*, Rule 71, comment 18.

volve making a series of defensive strikes in Afghanistan in response. The issue is that while international law grants states the right to self-defence against armed attacks, it also presumes that only states (or actors acting on behalf of states) can make armed attacks as a matter of law,[43] even if those non-state actors are "armed" in the sense of being able to mount the equivalent of an armed attack. While there are elements of state sovereignty over non-state actors, and state responsibility for their actions, there is not necessarily state culpability for the harm caused by non-state actors. Yet the right to self-defence may cause harm that, if not made in self-defence, would be a flagrant attack.

Consider a scenario where a technology hacking[44] group (perhaps a team of students doing a research project in a university course on power engineering), deciding it would be fun to see how resilient the North American electrical grid really is, gained control of the power distribution management systems in each region, including the interconnections between regions. Then imagine that the group started disconnecting high-voltage transmission lines from the grid. Suppose, too, that the operation is coordinated from a computer in New Zealand. The harm, even if it is inspired by technical curiosity rather than the desire to wreak industrial and commercial havoc, clearly has been caused by a non-state actor.[45] The group may be distributed, so each member of the group may be under the sovereignty of a different state. If this had been done by a state actor, a clear attribution could be made. But a state claiming the necessity of self-defence to end the threat would have only one plausible immediate target: the computer in New Zealand. Sending an uncrewed aerial vehicle (UAV) down the streets of Dunedin in search of a particular flat does not seem to be a minimum effective armed response—or even the response that ends the threat in the shortest time. An emergency throttling of Internet traffic through undersea and satellite interconnections would do. This action is permissible under state sovereignty,[46] could be requested by both Canadian and American

[43] *Tallinn 2.0*, Rule 71, comment 19.

[44] Here I mean *hacking* in the "figure out how it works" sense of the technical craft rather than the intentionally malevolent and criminal sense used in popular media.

[45] This kind of cyberoperation is not far-fetched. One of the goals of the US Cyber Command is to be able to take down the Russian electrical grid as an offensive measure should it be needed. Graff, "The Man Who Speaks Softly—and Commands a Big Cyber Army."

[46] *Tallinn 2.0*, Rule 62.

governments, and in the current context of intelligence partnerships, would likely be granted. But if the controlling computer had been in Ulaanbaatar, Mongolia, it is not clear that the isolation request could be honoured. Is a UAV attack then permissible, or is the appropriate response isolating North America from the global Internet until the threat can be contained?

The just-cause criteria set out in the *Tallinn Manual*'s assessment criteria for cyberattacks and the classification framework presented in this project will be useful in determining what degree of action may be justified in response to an attack by a non-state actor. The limiting factor is whether a state can justly respond to a non-state actor under the international laws of armed conflict rather than handling the threat under international criminal and commercial law.[47] In any case, a nocuous response must always be a last resort, after exhausting feasible moderate ones, with criminal and diplomatic methods following as quickly as practicable after the initial threat has been addressed. This still leaves open important questions about responsibility and reparations. To what extent can harm caused by non-state actors be attributed to states? If reparations are owed to the state hosting the non-state actor for harm caused in the course of responding to the initial attack, is it just to impose them on the targeted state? Does the hosting state owe reparations to the target state for an act that it did not commit but only had the obligation to stop once it became aware of it? Even though a state of armed conflict may not have existed between the states, some attenuated analogues to *jus post bellum* requirements might apply here, such as assurance of domestic criminal prosecution for the individuals responsible for the harm.

Information and technology concerns

Communication satellites

While there are very few civilians in space, there are many civilian objects in space, and those are primarily used for scientific and communication purposes. The *Tallinn Manual* draws a conceptual distinction between "space-enabled cyber operations and cyber-enabled space operations."[48] The latter applies to physical objects in space that are controlled by objects on the

[47] *Tallinn 2.0*, Rule 71, comment 18.

[48] *Tallinn 2.0*, 270.

ground, in the air, at sea, or in space.[49] These are subject to space-related treaties and international law concerning state sovereignty over and responsibility for objects owned by entities within the state registering the satellite.[50] The former applies primarily to the services provided by communication satellites such as SpaceX's Starlink system, which are elements of privately-owned network infrastructure that just happen to be in orbit. The communication facilitated by these satellites, and to some degree the satellites as physical components of the global communication infrastructure, are governed under international telecommunications treaties[51] and other conventionally accepted international laws.[52]

As physical objects, communication satellites often serve both civil and military purposes.[53] However, treaties governing the use of outer space permit the use of space for peaceful purposes only.[54] In other words, satellites may be used for military purposes only if they are not facilitating the use of force (moderate or nocuous) or the transgression of international law (self-defence and UN Security Council licence might be exceptions as long as the satellites themselves are not weapons). But any military use, even for non-combat purposes, makes them lawful targets during times of international armed conflict,[55] just as dual-purpose terrestrial communications facilities are. Thus satellites serving purely civilian purposes would have protected status under the laws of armed conflict as long as they are not providing services for military activity.[56]

Launching a strike against any object in space (whether in self-defence or during an international armed conflict) cannot be undertaken without a consideration of what the collateral effects are likely to be.[57] The physical destruction of any satellite would create a debris field that might interfere with other satellites.[58] Altering the orbit or orientation of a satellite used for both

[49] *Tallinn 2.0*, 271.
[50] *Tallinn 2.0*, Rule 58, comment 1.
[51] *Tallinn 2.0*, 284.
[52] *Tallinn 2.0*, Rule 58, comment 8.
[53] *Tallinn 2.0*, Rule 58, comment 7.
[54] *Tallinn 2.0*, Rule 58.
[55] *Tallinn 2.0*, Rule 101.
[56] *Tallinn 2.0*, Rule 58, comment 11.
[57] *Tallinn 2.0*, Rule 113, comments 3, 6.
[58] *Tallinn 2.0*, Rule 58, comments 5, 11.

military and civilian purposes ends the provision of service to both. The former is nocuous, with secondary harm likely to occur on occasion for years afterward. The second is a moderate response, since it does disrupt civilian service and is not likely to have harmful second-order effects. Regardless of the severity of the planned response, the direct and indirect effects must both be accounted for when assessing the proportionality constraint on possible uses of force. Any measures taken against communication satellites or other objects in space must be necessary to achieve the specific military objective, without producing excessive collateral damage to civilian objects.[59] However, as the ICRC notes, most data communication technologies have redundant routes; if one route (say, a satellite connection) is blocked, another route will be chosen (possibly involving another satellite).[60] Completely cutting off communication would require disabling every possible route, and so every satellite capable of carrying data traffic would need to be taken out of service somehow, along with every terrestrial connection. This quickly becomes an infeasible way of meeting the military objective of stopping data communication to and from an adversary state. The indefinite valuation of, for example, the loss of government services available only over the Internet or the disruption to global transportation infrastructure adds further complexity to the proportionality assessment. Moreover, this assessment must be made before the strike is launched, since an after-the-fact determination of proportionality defeats the purpose of the obligation.[61]

It is always going to be difficult to perform a proportionality analysis with respect to communication satellites. One of the simultaneously fascinating and maddening characteristics of networked computing and communications systems is that while failure modes of individual components and the follow-on effects are typically well-understood, the effects that such failure has on other parts of the infrastructure depends on how the surviving elements interact as they respond individually to the disruption. This emergent collective behaviour makes it difficult to assess the extent of any indirect effects resulting from an attack on cyber infrastructure. The skill in simulating, analyzing, and understanding these cascading failures has to be developed before this kind of disruption can be ruled out of the proportion-

[59] *Tallinn 2.0*, Rule 113.

[60] International Committee of the Red Cross (ICRC), "Challenges of Contemporary Armed Conflict (2015)," 42.

[61] *Tallinn 2.0*, Rule 113, comment 11.

ality assessment. Until there is a reasonable judgement that can be made to the contrary, any attack on a communications satellite should be expected to produce wide-spread communication chaos and disruption of economic activity in non-belligerent states, not just the target state.

In principle, then, while disabling a communication satellite may be permissible under the laws of armed conflict, the state of knowledge concerning the extent of plausible collateral harm mitigates against it, and other, lower-risk means of disabling military use of communication satellites—such as targeting military ground stations—appear to be favoured. How much modelling of effects is "good enough" to justify a strike against the satellite itself? When is the epistemic burden of assessing potential effects reasonably satisfied, and how can that be demonstrated before the fact?

Data as objects

Chapter 6 discusses the need to protect data needful to rebuild and sustain civil society and cultural heritage. I have not addressed the idea of data as property and how to assess the harm incurred through its loss. This question is now more relevant than ever in an economy driven by the automated interpretation of data.

Any medium containing data is tangible property that can be owned. Data objects themselves are intangible, but they have information content that may also be owned and assigned economic value; the notion of intellectual property is evidence that data can be property. While businesses and governments understand this well, and most of them take steps to safeguard their data from loss or alteration, this comes at the cost of acquiring and maintaining a data management infrastructure. The advent of so-called *cloud-based services*[62] provides an opportunity to contract out these data management functions for a lower cost, at the risk of entrusting data to another organization. This, in turn, opens up a new area of insurable risk: the liability for loss of customers' data.[63]

[62] The name derives from the convention of representing the global Internet and its potential "someone else can do this" commodity services in network diagrams as an indistinct complexity-obscuring cloud.

[63] Marianne Bonner, "Liability for Damage to Electronic Data," *The Balance Small Business*, December 8, 2018, accessed October 16, 2020, `https://www.thebalancesmb.com/liability-for-damage-to-electronic-data-462620`.

In this regard, data is much like money. Both are intangible though representable in multiple media forms; both have economic value; both are objects of fiduciary duties and liabilities; both can be created, lost, and destroyed. A banknote or a coin is a document asserting that it has a fixed monetary value. But only money in the form of currency and in the hands of non-combatants (civilians, prisoners of war, internees, the shipwrecked, wounded, sick, or dead) has protection under the laws of armed conflict.[64] (Currency in the hands of a belligerent state is likely to be used, at least in part, for military purposes and so may be lawfully targeted.) However, the total wealth of the world is not represented entirely in currency or precious metal. It is represented in account records as data, now largely stored in digital form. Time may not be money, but money is data. If all rights- and culture-supporting digital data is accorded the same reverence as the wealth represented in digital form, there would be more clarity around relevant protections for these kinds of data during both times of armed conflict and of peace. Further, wealth is instrumental to the enjoyment of rights and the development of culture. It seems a little backward to afford the thing with merely instrumental value more protection than the things of plausible intrinsic value to which it facilitates access.

This comes back to the discussion in Chapter 5 about the IMF's interest in securing financial data. If that can be secured, then any other data relevant to state interests, including human rights, can also be secured. The point here is that, as the physical objects that carry information about intangible objects change, the concept of *object* has to change as well. Again, the ICRC has the right of it: "the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them."[65] Classifying money as one type of data opens the way to identifying other types of data, each of which can be subject to its own level of protection as the international community sees fit. Philosophically this continues the conversation about the metaphysics of information and economics.

[64] GC I, Art. 16; GC II, Art. 19; GC III, Art. 18; GC IV, Art. 97; AP I, Art. 52; AP II, Art. 13.
[65] Challenges of Contemporary Armed Conflict (2019), 28.

7.3 Value of this part of the project

Cyberwarfare opens up a new way for states to interfere in the sovereign affairs of other states. My dissertation project has argued for the value of the *Tallinn Manual* and provided an analysis of its interpretation of the international laws of armed conflict with respect to cyberoperations. I have set out conceptual frameworks for assessing the causal chain, timing, extent of the effects, and severity of permissible responses associated with being the target of an aggressive cyberoperation. Since cyberwarfare, as any other kind of warfare, poses risks to the civilian population and the record of human heritage, I thought it important to examine the protections that international law provides during times of armed conflict and the steps toward implementing those protections during times of peace. I have identified and described a gap in the articulation of protections afforded to civilian data objects, be they digital or physical, under international law, and argued that protecting these data objects is essential for the safeguarding of human rights. In response I have developed some guidance on how states could protect these objects from damage or loss by cyber or conventional means. Constraining the effects of aggressive cyberoperations is, then, just as important as constraining the effects of war conducted by other means, and the international community ought to continue working toward agreement on how to do this. Finally, I have set out how this work can be continued and connected to questions in metaphysics, epistemology, and applied ethics with respect to human rights. I trust that this dissertation has also made a constructive contribution to philosophy as a discipline. May humanity be better for it.

Letter of copyright permission

From: misha@evstafiev.com
Subject: Re: Inclusion of a photograph in a dissertation
Date: March 20, 2021 at 4:44 AM
To: Jim Jordan wjjordan@uwaterloo.ca

Thank you for asking, Jim.

Please go ahead, and good luck with the presentation.

best, Mikhail

> On March 20, 2021 1:35 AM Jim Jordan <wjjordan@uwaterloo.ca> wrote:
>
> Dear Mr. Evstafiev:
>
> I am writing a doctoral dissertation on cyberwarfare and its potential effects on cultural heritage. In my 3-Minute Thesis presentation I used your photograph of Vedran Smailović, "The Cellist of Sarajevo," as the static visual element. I am incorporating the transcript of the presentation as an appendix to my dissertation and would like to include the photograph at https://en.wikipedia.org/wiki/Vedran_Smailović#/media/File:Evstafiev-bosnia-cello.jpg without risking the dissertation being placed under the CC BY-SA 3.0 licence.
>
> May I please have your permission to include the photograph in the dissertation? I will, of course, include attribution and a reference to the CC BY-SA 3.0 licence, but also add a note indicating that I am using it under explicit permission from the creator.
>
> Thank you for your consideration. I look forward to hearing from you soon.
>
> With regards,
>
> W. Jim Jordan
>
> --
> W. Jim Jordan (he/him)
> PhD candidate, Department of Philosophy, University of Waterloo
> E-mail: wjjordan@uwaterloo.ca Office: HH 364
>
> I acknowledge that I live and work on the traditional territory of the Neutral, Anishnaabeg and Haudenosaunee peoples. The University of Waterloo is situated on the Haldimand Tract, the land promised to the Six Nations that includes six miles on each side of the Grand River.
>
> Any email from this account received outside of teaching hours likely isn't important enough to merit an immediate response. It can wait until an appropriate time.

Mikhail Evstafiev

www.evstafiev.com

Bibliography

Books

Besson, Samantha, and John Tasioulas, eds. *The Philosophy of International Law*. Oxford, UK: Oxford University Press, 2010.

Bowett, Derek William. *Self-Defence in International Law*. New York, NY: Frederick A. Praeger, 1958.

Carr, Jeffrey. *Inside Cyber Warfare*. 2nd ed. Sebastopol, CA: O'Reilly Media, 2011.

Clapham, Andrew, Paola Gaeta, Tom Haeck, and Alice Priddy, eds. *The Oxford Handbook of International Law in Armed Conflict*. Oxford, UK: Oxford University Press, 2014.

Commission of the European Communities. *Communication from the Commission on a European Program for Critical Infrastructure Protection*. COM(2006) 786. Brussels, BE, December 12, 2006. Accessed August 15, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN.

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy and National Research Council [USA], eds. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: National Research Council [USA], The National Academies Press, June 10–11, 2010. http://www.nap.edu/catalog/12997/proceedings-of-a-workshop-on-deterring-cyberattacks-informing-strategies-and.

Committee on Offensive Information Warfare, Computer Science and Telecommunications Board, and National Research Council [USA]. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Edited by William A. Owens, Kenneth W. Dam, and Herbert S. Lin. Washington, DC: The National Academies Press, 2009. http://www.nap.edu/catalog/12651/technology-policy-law-and-ethics-regarding-us-acquisition-and-use-of-cyberattack-capabilities.

Department of Defense [USA]. *Department of Defense Law of War Manual*. December 13, 2016. Accessed May 1, 2019. https://www.hsdl.org/?view&did=797480.

Department of Defense [USA]. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (As Amended through 15 June 2015)*. June 15, 2015. Accessed October 23, 2015. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Department of Defense [USA]. *Joint Publication 3-13.2: Psychological Operations*. January 7, 2010. Accessed February 5, 2021. https://fas.org/irp/doddir/dod/jp3-13-2.pdf.

———. *Strategy for Operating in Cyberspace*. July 2011. Accessed September 9, 2019. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Evans, Gareth, Mohamed Sahnoun, Gisèle Côté-Harper, Lee Hamilton, Michael Ignatieff, Vladimir Lukin, Klaus Naumann, et al. *The Responsibilty to Protect: Report of the International Commission on Intervention and State Sovereignty*. Ottawa, ON: International Development Research Centre, 2001.

Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa, ON: Public Safety Canada, 2010. Accessed September 9, 2019. http://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf.

Great Britain Cabinet Office. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London, UK: The Stationary Office, October 18, 2010. Accessed September 9, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

Halpin, Edward, Philippa Trevorrow, David Webb, and Steve Wright, eds. *Cyberwar, Netwar, and the Revolution in Military Affairs*. Basingstoke, UK: Palgrave MacMillan, 2006.

Instittute of International Law (IIL). Manual of the Laws of Naval War, August 9, 1913. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/0F63D17A90E5CDC0C12563CD002D68EF/FULLTEXT/IHL-33-EN.pdf.

———. The Laws of War On Land, September 9, 1880. Accessed January 1, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/40371257507EBB71C12563CD002D6676/FULLTEXT/IHL-8-EN.pdf.

International Committee of the Red Cross (ICRC). *Commentary on the First Geneva Convention: Convention (1) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. 2nd ed., edited by Knut Dörmann, Liesbeth Lijnzaad, Marco Sassòli, and Philip Spoerri. March 22, 2016. Accessed October 2, 2019. https://ihl-databases.icrc.org/ihl/full/GCI-commentary.

———. *Customary International Humanitarian Law*. Edited by Jean-Marie Henckaerts and Louise Doswald-Beck. 2 vols. Cambridge, UK: Cambridge University Press, 2005.

International Institute of Humanitarian Law. *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, edited by Louise Doswald-Beck. Cambridge, UK: Cambridge University Press, 1985.

Jordan, W. Jim, Andrew Stumpf, Chris Wass, Vanessa Correia, Dylon McChesney, Jamie Sewell, and Sara Weaver. *With a Clear Conscience: Business Ethics, Decision-Making, and Strategic Thinking*. Edited by Gregory G. Andres. Don Mills, ON: Oxford University Press, 2021.

Kalshoven, Frits, and Liesbeth Zegveld. *Constraints on the Waging of War: An Introduction to International Humanitarian Law*. 4th ed. Cambridge, UK: Cambridge University Press. Accessed December 30, 2020. https://shop.icrc.org/constraints-on-the-waging-of-war-an-introduction-to-international-humanitarian-law-pdf-en.

Knuth, Rebecca. *Libricide: The Regime-Sponsored Destruction of Books and Libraries in the Twentieth Century*. Westport, CT: Greenwood Publishing Group, 2003.

National Research Council [USA]. *Building an Electronic Records Archive at the National Archives and Records Administration: Recommendations for a Long-Term Strategy*. Edited by Robert F. Sproull and John Eisenberg. Washington, DC: The National Academies Press, 2005.

Reed, Thomas C. *At the Abyss: An Insider's History of the Cold War*. New York, NY: Ballantine Books, 2005.

Reychler, Luc. *Time for Peace: The Essential Role of Time in Conflict and Peace Processes*. Brisbane, AU: University of Queensland Press, 2015.

Russian Federation. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. Translated by NATO CCD COE. Unofficial translation. 2011. Accessed September 9, 2019. http://ccdcoe.eu/uploads/2018/10/Russian_Federation_unofficial_translation.pdf.

Sandoz, Yves, Christophe Swinarski, and Bruno Zimmermann, eds. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva, CH: Martinus Nijhoff, 1987. Accessed January 6, 2016. http://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge, UK: Cambridge University Press, 2013. Accessed September 18, 2015. http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

Schmitt, Michael N., and Liis Vihul, eds. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge, UK: Cambridge University Press, 2017.

Suzor, Nicholas P. *Lawless: The Secret Rules That Govern Our Digital Lives*. Cambridge, UK: Cambridge University Press, 2019.

The Program on Humanitarian Policy and Conflict Research at Harvard University. *HPCR Manual on International Law Applicable to Air and Missile Warfare*. New York, NY: Cambridge University Press, 2013.

Uhler, Oscar M., Henri Coursier, Frédéric Siordet, Claude Pilloud, Roger Boppe, René-Jean Wilhelm, and Jean-Pierre Schoenholzer. *Commentary: IV Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, edited by Jean S. Pictet, translated by Ronald Griffin and C. W. Dumbleton, vol. 4. The Geneva Conventions of 12 August 1949. Geneva, CH: International Committee of the Red Cross (ICRC), 1958. Accessed January 8, 2021. https://b-ok.org/book/1266129/0a8d8d.

Yannakogeorgos, Panayotis A., and Adam B. Lowther, eds. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton, FL: Taylor & Francis, 2013.

Book chapters

Darnton, Geoffrey. "Information Warfare and the Laws of War." Chap. 9 in Halpin, Trevorrow, Webb, and Wright, *Cyberwar, Netwar, and the Revolution in Military Affairs*, 139–153.

Dipert, Randall R. "The Essential Features of an Ontology for Cyberwarfare." Chap. 5 in Yannakogeorgos and Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 35–48.

Dunlap, Charles J., Jr. "Perspectives for Cyberstrategists on Cyberlaw for Cyberwar." Chap. 13 in Yannakogeorgos and Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 211–232.

Lukasik, Stephen J. "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains." In Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy and National Research Council [USA], *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 99–121.

Moran, Ned. "A Cyber Early Warning Model." Chap. 12 in Carr, *Inside Cyber Warfare*, 179–189.

Nowak, Manfred. "Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment." Chap. 16 in Clapham, Gaeta, Haeck, and Priddy, *The Oxford Handbook of International Law in Armed Conflict*, 387–409.

Oliver, Eric P. "Stuxnet: A Case Study in Cyber Warfare." Chap. 10 in Yannakogeorgos and Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 127–160.

Orend, Brian D. "War." In *Stanford Encyclopedia of Philosophy*, Spring 2016, edited by Edward N. Zalta. July 28, 2005. Accessed October 27, 2015. `http://plato.stanford.edu/archives/fall2008/entries/war/`.

Schmitt, Michael N. "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts." In Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy and National Research Council [USA], *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 151–178.

Shue, Henry. "Laws of War." Chap. 25 in Besson and Tasioulas, *The Philosophy of International Law*, 511–527.

Song, Sarah. "The Subject of Multiculturalism: Culture, Religion, Language, Ethnicity, Nationality, and Race?" Chap. 10 in *New Waves in Political Philosophy*, 177–197. Basingstoke, UK: Palgrave MacMillan, 2009.

Armstead, J. Holmes, Jr. "The International Criminal Court: History, Development and Status." *Santa Clara Law Review* 38, no. 3 (January 1998): 745–835. Accessed January 7, 2021. http://digitalcommons.law.scu.edu/lawreview/vol38/iss3/3.

Balakian, Peter. "Raphael Lemkin, Cultural Destruction, and the Armenian Genocide." *Holocaust and Genocide Studies* 27, no. 1 (Spring 2013): 57–89.

Barrett, Edward T. "Reliable Old Wineskins: The Applicability of the Just War Tradition to Military Cyber Operations." *Philosophy & Technology* 28 (September 2015): 387–405.

Boer, Lianne J. M. " 'Restating the Law "As It Is" ': On the Tallinn Manual and the Use of Force in Cyberspace." *Amsterdam Law Forum* 5, no. 3 (Summer 2013): 4–18. Accessed January 25, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2338066.

Colvin, Chris, Daniel B. Garrie, and Siddartha Rao. "Cyber Warfare and the Corporate Environment." *Journal of Law & Cyber Warfare* 2, no. 1 (Spring 2013): 1–24. Accessed January 25, 2021. https://www.jlcw.org/wp-content/uploads/2016/09/2013-JLCW-SpringVol_2_1.pdf.

Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4 (December 16, 2010): 384–410. https://doi.org/10.1080/15027570.2010.536404.

Fal', O.M. "Standardization in Information Technology Security." *Cybernetics and Systems Analysis* 53, no. 1 (January 2017): 78–82. https://doi.org/10.1007/s10559-017-9908-8.

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Global Politics and Strategy* 53, no. 1 (January 28, 2011): 23–40. https://doi.org/10.1080/00396338.2011.555586.

Ghafur, Saira, Soren Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin. "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS." *npj Digital Medicine* 2, no. 98 (October 2, 2019): 1–7. Accessed December 20, 2020. https://doi.org/10.1038/s41746-019-0161-6.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs* 86, no. 2 (March 2010): 523–541. https://doi.org/10.1111/j.1468-2346.2010.00894.x.

Jenkins, Ryan. "Is Stuxnet Physical? Does it Matter?" *Journal of Military Ethics* 12, no. 1 (April 17, 2013): 68–79. https://doi.org/10.1080/15027570.2013.782640.

Kennedy, David. "The Sources of International Law." *American University International Law Review* 2, no. 1 (March 1987): 1–96. Accessed January 25, 2021. https://digitalcommons.wcl.american.edu/auilr/vol2/iss1/1/.

Kymlicka, Will. "Multiculturalism and Minority Rights: West and East." *Journal on Ethnopolitics and Minority Issues in Europe* 3, no. 4 (2002): 1–24.

———. "National Cultural Autonomy and International Minority Rights Norms." *Ethnopolitics* 6, no. 3 (September 2007): 373–393.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (August 2013): 365–404. https://doi.org/10.1080/09636412.2013.816122.

McGhee, James E. "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy." *Journal of Law & Cyber Warfare* 2, no. 1 (Spring 2013): 64–103. Accessed January 25, 2021. https://www.jlcw.org/wp-content/uploads/2016/09/2013-JLCW-SpringVol_2_1.pdf.

Orend, Brian D. "Justice after War." *Ethics & International Affairs* 16, no. 1 (March 2002): 43–56. Accessed October 25, 2015. https://doi.org/10.1111/j.1747-7093.2002.tb00374.x.

Pierce, Albert C. "Just War Principles and Economic Sanctions." *Ethics and International Affairs* 10 (March 1996): 99–113. https://doi.org/10.1111/j.1747-7093.1996.tb00005.x.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Riedlmayer, András J. "Crimes of War, Crimes of Peace: Destruction of Libraries during and after the Balkan Wars of the 1990s." *Library Trends* 56, no. 1 (Summer 2007): 107–132.

Sassòli, Marco. "State Responsibility for Violations of International Humanitarian Law." *Revue Internationale de la Croix Rouge* 84, no. 846 (June 2002): 401–34. Accessed December 11, 2020. https://www.icrc.org/en/doc/assets/files/other/401_434_sassoli.pdf.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37, no. 3 (1999): 885–938. https://heinonline.org/HOL/Page?handle=hein.journals/cjtl37&id=893.

———. "Cyberspace and International Law: The Penumbral Mist of Uncertainty." *Harvard Law Review Forum* 126, no. 5 (March 2013): 176–180. Accessed January 25, 2021. https://harvardlawreview.org/wp-content/uploads/pdfs/forvol126_schmitt.pdf.

———. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal* 54 (December 2012): 13–37. Accessed January 25, 2021. https://harvardilj.org/wp-content/uploads/sites/15/2012/12/HILJ-Online_54_Schmitt.pdf.

Segal, Adam M. "Cyberspace: The New Strategic Realm in US-China Relations." *Strategic Analysis* 38, no. 4 (July 2014): 577–581. https://doi.org/10.1080/09700161.2014.918447.

Singer, Peter W. "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons." *Case Western Reserve Journal of International Law* 47, no. 1 (Spring 2015): 79–86. Accessed December 27, 2020. https://scholarlycommons.law.case.edu/jil/vol47/iss1/10.

Woods, Robin. "Report on National Program Archives." *ARSC Journal* 2, nos. 2/3 (Spring–Summer 1970): 3–23. Accessed April 1, 2019. http://www.arsc-audio.org/journals/v2/v02n2-3p3-23.pdf.

Treaties, conventions, protocols, charters, and resolutions

Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal, London, August 8, 1945. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/87B0BB4A50A64DEAC12563CD002D6AAE/FULLTEXT/IHL-49-EN.pdf.

Blue Shield. *Amendment to the Articles of Association: Association of National Committees of the Blue Shield*. Amsterdam, NL, April 6, 2015. Accessed March 5, 2021. https://theblueshield.org/wp-content/uploads/2018/06/statute-Amendments_BSI_2016.pdf.

Conference for the Supervision of the International Trade in Arms and Ammunition. Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, Geneva, June 17, 1925. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/921B4414B13E58B8C12563CD002D693B/FULLTEXT/IHL-36-EN.pdf.

Council of Europe. Convention on Cybercrime, November 23, 2001, ETS 185. Accessed November 24, 2020. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, December 11, 1868. Accessed December 31, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/3C02BAF088A50F61C12563CD002D663B/FULLTEXT/IHL-6-EN.pdf.

Hague Peace Conferences. Convention (II) Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, July 29, 1899. Accessed January 1, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/CD0F6C83F96FB459C12563CD002D66A1/FULLTEXT/IHL-10-EN.pdf.

———. Convention (II) with Respect to the Laws and Customs of War on Land, The Hague, July 29, 1899. Accessed January 1, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/CD0F6C83F96FB459C12563CD002D66A1/FULLTEXT/IHL-10-EN.pdf.

———. Convention (III) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention of 22 August 1864, The Hague. Accessed January 3, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2B134D111958C73AC12563CD002D66C8/FULLTEXT/IHL-11-EN.pdf.

———. Convention (IV) Respectting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, October 18, 1907. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/4D47F92DF3966A7EC12563CD002D6788/FULLTEXT/IHL-19-EN.pdf.

———. Convention (IX) Concerning Bombardment by Naval Forces in Time of War, The Hague, October 18, 1907. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/F13F9FFC628FC33BC12563CD002D6819/FULLTEXT/IHL-24-EN.pdf.

———. Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, October 18, 1907. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/71929FBD2655E558C12563CD002D67AE/FULLTEXT/IHL-20-EN.pdf.

Hague Peace Conferences. Convention (VIII) Relative to the Laying of Automatic Submarine Contact Mines, The Hague, October 18, 1907. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/7D389CA23C22337BC12563CD002D67FF/FULLTEXT/IHL-23-EN.pdf.

———. Convention (X) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention, The Hague, October 18, 1907. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/E5397A0FB560D0A9C12563CD002D6832/FULLTEXT/IHL-25-EN.pdf.

———. Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, The Hague, October 18, 1907. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/06A47A50FE7412AFC12563CD002D6877/FULLTEXT/IHL-28-EN.pdf.

———. Declaration (IV,2) Concerning Asphyxiating Gases, The Hague, July 29, 1899. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/B0625F804A9B2A64C12563CD002D66FF/FULLTEXT/IHL-13-EN.pdf.

———. Declaration (IV,3) Concerning Expanding Bullets, The Hague, July 29, 1899. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/D528A73B322398B5C12563CD002D6716/FULLTEXT/IHL-14-EN.pdf.

International Committee of the Red Cross (ICRC). Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, August 12, 1949, 75 UNTS 31. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/4825657B0C7E6BF0C12563CD002D6B0B/FULLTEXT/GC-I-EN.pdf.

———. Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva, August 12, 1949, 75 UNTS 85. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2F5AA9B07AB61934C12563CD002D6B25/FULLTEXT/GC-II-EN.pdf.

———. Convention (III) Relative to the Treatment of Prisoners of War, Geneva, August 12, 1949, 75 UNTS 135. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/77CB9983BE01D004C12563CD002D6B3E/FULLTEXT/GC-III-EN.002.pdf.

———. Convention (IV) Relative to the Protection of Civilian Persons in Time of War. Geneva, August 12, 1949, 75 UNTS 287. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/AE2D398352C5B028C12563CD002D6B5C/FULLTEXT/ATTXSYRB.pdf.

———. Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, July 6, 1906. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/C64C3E521F5CC28FC12563CD002D6737/FULLTEXT/IHL-GC-1906-EN.pdf.

———. Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, July 27, 1929. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/09DFB7A98E19533AC12563CD002D6997/FULLTEXT/IHL-GC-1929-1-EN.pdf.

———. Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Geneva, August 22, 1864. Accessed December 28, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/477CEA122D7B7B3DC12563CD002D6603/FULLTEXT/IHL-GC1864-EN.pdf.

International Committee of the Red Cross (ICRC). Convention Relative to the Treatment of Prisoners of War, Geneva, July 27, 1929. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/0BDEDDD046FDEBA9C12563CD002D69B1/FULLTEXT/IHL-GC-1929-2-EN.pdf.

———. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem (Protocol III), Geneva, December 8, 2005. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/8BC1504B556D2F80C125710F002F4B28/FULLTEXT/AP-III-EN.pdf.

———. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Geneva, June 8, 1977, 1125 UNTS 3. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/D9E6B6264D7723C3C12563CD002D6CE4/FULLTEXT/AP-I-EN.pdf.

———. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), Geneva, June 8, 1977, 1125 UNTS 609. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/AA0C5BCBAB5C4A85C12563CD002D6D09/FULLTEXT/AP-II-EN.pdf.

International Council on Archives (ICA). *Constitution*, August 24, 2012. Accessed April 21, 2018. https://www.ica.org/sites/default/files/constitution_2012_en_final_2016_visual_identity.pdf.

International Criminal Court (ICC). Rome Statute of the International Criminal Court, 2011, 2187 UNTS 90, amended, The Hague, NL. Accessed April 8, 2020. https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf.

Pan-American Union. Treaty on the Protection of Artistic and Scientific Institutions and Historic Monuments (Roerich Pact), Washington, 15 April 1935, April 15, 1935. Accessed January 3, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/EE57F295093E44A4C12563CD002D6A3F/FULLTEXT/IHL-44-EN.pdf.

Project of an International Declaration Concerning the Laws and Customs of War, Brussels, August 27, 1874. Unratified. Accessed January 1, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/42F78058BABF9C51C12563CD002D6659/FULLTEXT/IHL-7-EN.pdf.

Shanghai Cooperation Organization. Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, June 16, 2009. Unofficial translation. Accessed November 25, 2020. http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf.

Treaty for the Limitation and Reduction of Naval Armaments, (Part IV, Art. 22, relating to submarine warfare), London, April 22, 1930. Accessed January 4, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/32C5DA6C8C43775AC12563CD002D69CC/FULLTEXT/IHL-41-EN.pdf.

United Nations. Charter of the United Nations, October 24, 1945, 1 UNTS XVI. Accessed October 6, 2015. http://www.refworld.org/docid/3ae6b3930.html.

———. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Geneva, October 10, 1980, 1342 UNTS 137. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/7A690F9945FF9ABFC12563CD002D6D8E/FULLTEXT/IHL-81-EN.pdf.

———. Convention on the Law of the Sea, December 10, 1982, 1833 UNTS 3. Accessed November 28, 2019. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

United Nations. Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, December 10, 1976, 1108 UNTS 151. Accessed November 26, 2019. https://treaties.un.org/doc/Treaties/1978/10/19781005%2000-39%20AM/Ch_XXVI_01p.pdf.

———. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, London, Moscow and Washington, April 10, 1972, 1015 UNTS 163. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/BACF97285A9CB2A2C12563CD002D6C88/FULLTEXT/IHL-68-EN.pdf.

———. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Paris, January 13, 1993, 1974 UNTS 45. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/9D3CCA7B40638EF5C12563F6005F63C5/FULLTEXT/IHL-87-EN.pdf.

———. Protocol on Blinding Laser Weapons (Protocol IV) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, October 13, 1995, 2024 UNTS 163. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/70D9427BB965B7CEC12563FB0061CFB2/FULLTEXT/IHL-91-EN.pdf.

———. Protocol on Explosive Remnants of War (Protocol V) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, November 28, 2003, 2399 UNTS 100. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/22EFA0C23F4AAC69C1256E280052A81F/FULLTEXT/IHL-99-EN.pdf.

———. Protocol on Non-Detectable Fragments (Protocol I) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, October 10, 1980, 1342 UNTS 168. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/CFCC9F92E14E1945C12563CD002D6DA9/FULLTEXT/IHL-82-EN.pdf.

———. Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons (Protocol III) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, October 10, 1980, 1342 UNTS 171. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/1E37E38A51A1941DC12563CD002D6DEA/FULLTEXT/IHL-84-EN.pdf.

———. Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices As Amended (Protocol II Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects), May 3, 1996, 2048 UNTS 93. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/82CF2C7C75E37C5AC12563FB006181B4/FULLTEXT/IHL-92-EN.pdf.

———. Statute of the International Court of Justice, June 26, 1945, Can TS 7 (1945). Accessed January 28, 2021. https://www.icj-cij.org/en/statute.

———. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, January 27, 1967, 610 UNTS 205. Accessed November 28, 2019. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

United Nations. Treaty on the Prohibition of Nuclear Weapons, July 7, 2017. Accessed December 19, 2020. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/209/73/PDF/N1720973.pdf.

United Nations Educational, Scientific and Cultural Organization (UNESCO). Convention for the Protection of Cultural Property in the Event of Armed Conflict, The Hague, May 14, 1954, 249 UNTS 215. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2A07EB0EAA5CECACC12563CD002D6BC8/FULLTEXT/IHL-60-EN.pdf.

———. Convention for the Safeguarding of the Intangible Cultural Heritage, Paris, October 17, 2003. Accessed March 4, 2021. https://ich.unesco.org/en/convention.

———. Protocol for the Protection of Cultural Property in the Event of Armed Conflict, The Hague, May 14, 1954, 249 UNTS 358. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/79B801B4D23AEA95C12563CD002D6BE3/FULLTEXT/IHL-61-EN.pdf.

———. Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict, The Hague, March 26, 1999, 2253 UNTS 172. Accessed April 17, 2017. http://unesdoc.unesco.org/images/0013/001306/130696eo.pdf.

United Nations General Assembly. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, December 10, 1984, 1465 UNTS 85. Accessed January 5, 2021. https://www.ohchr.org/Documents/ProfessionalInterest/cat.pdf.

———. Convention on the Rights of the Child, November 20, 1989, 1577 UNTS 3. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/B92BDC3CAE1B142DC12563CD002D6E8C/FULLTEXT/IHL-86-EN.pdf.

———. "Definition of Aggression." Resolution 3314 (XXIX), December 14, 1974. Accessed January 30, 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX).

———. International Covenant on Civil and Political Rights, December 16, 1966, 999 UNTS 171. Accessed February 12, 2019. https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf.

———. International Covenant on Economic, Social and Cultural Rights, December 16, 1966, 993 UNTS 3. Accessed June 26, 2018. https://treaties.un.org/doc/Treaties/1976/01/19760103%2009-57%20PM/Ch_IV_03.pdf.

———. Universal Declaration of Human Rights, December 10, 1948, A/RES/217(III). Accessed January 5, 2021. https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

United Nations Human Rights Committee. "Status of Ratification Interactive Dashboard," April 15, 2019. Accessed April 16, 2019. http://indicators.ohchr.org.

United Nations Human Rights Council. Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, June 30, 2016, A/HRC/32/L.20. Accessed February 11, 2021. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

United Nations International Law Commission. "Draft Articles on Responsibility of States for Internationally Wrongful Acts." Supplement No. 10 (A/56/10), ch. IV.E.1, November 2001. Accessed December 11, 2020. https://legal.un.org/ilc/reports/2001/english/chp4.pdf.

United States of America. "Instructions for the Government of Armies of the United States in the Field (Lieber Code)," April 24, 1863. Accessed December 28, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/A25AA5871A04919BC12563CD002D65C5/FULLTEXT/IHL-L-Code-EN.pdf.

Cases

International Court of Justice (ICJ). *Corfu Channel case*, 1949 ICJ 4, April 9, 1949. Accessed April 25, 2016. http://www.icj-cij.org/docket/files/1/1645.pdf.

International Court of Justice (ICJ). *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 1996 ICJ 226, July 8, 1996. Accessed November 24, 2015. http://www.icj-cij.org/docket/files/95/7495.pdf.

———. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua* v. *United States of America)*, 1986 ICJ 14, June 27, 1986. Accessed October 13, 2015. http://www.icj-cij.org/docket/files/70/6503.pdf.

International Criminal Tribunal for the Former Yugoslavia (ICTY). *Milutinović case* (appeal judgement), IT-05-87-A, January 23, 2014. Accessed March 20, 2019. http://www.icty.org/x/cases/milutinovic/acjug/en/140123.pdf.

———. *Milutinović case* (judgement), IT-05-87-T, February 26, 2009. Accessed March 20, 2019. http://www.icty.org/x/cases/milutinovic/tjug/en/jud090226-e3of4.pdf.

———. *Milutinović case* (redacted third amended joinder indictment), IT-05-87-PT D6404, June 21, 2006. Accessed March 20, 2019. http://www.icty.org/x/cases/milutinovic/ind/en/milutinovic_060621e.pdf.

Permanent Court of International Justice (PCIJ). *The Case of the ss* Lotus *(France v. Turkey)*, 1927 PCIJ (ser. A) 10, September 7, 1927. Accessed November 24, 2020. http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm.

Technical standards

ASTM International. *Standard Guide for Cybersecurity and Cyberattack Mitigation*. Technical standard. F3286-17. West Conshohocken, PA: ASTM International, December 1, 2017. Accessed September 1, 2020. https://doi.org/10.1520/F3286-17.

———. *Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems in Accordance with IMO Resolution MSC.428(98)—Cyber Risks and Challenges*. Technical standard. F3449-20. West Conshohocken, PA: ASTM International, June 1, 2020. Accessed September 1, 2020. https://doi.org/10.1520/F3449-20.

———. *Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)*. Technical standard. F3201-16. West Conshohocken, PA: ASTM International, September 1, 2016. Accessed September 1, 2020. https://doi.org/10.1520/F3201-16.

Common Criteria. *Common Criteria for Information Technology Security Evaluation*. Version 3.1, Revision 5. April 2017. Accessed October 29, 2019. https://www.commoncriteriaportal.org/cc/.

Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System (OAIS): Recommended Practice*. 2nd ed. CCSDS 650.0-M-2. Washington, DC, June 2012. Accessed March 6, 2021. https://public.ccsds.org/Pubs/650x0m2.pdf.

International Organization for Standardization and International Electrotechnical Commission. *International Standard ISO/IEC 27000: Information Technology—Security Techniques—Information Security Management Systems*. Technical standard. ISO/IEC 27000:2018(E). Geneva, CH: International Organization for Standardization, February 2018. https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip.

News reports and commentaries

Acker, Fabian. "Fatal Failures: Siberia's Hydro Disaster." *Engineering and Technology Magazine* 6, no. 7 (July 11, 2011). Accessed March 28, 2016. http://eandt.theiet.org/magazine/2011/07/siberia-hydro-disaster.cfm.

Adams, Michael J. "A Warning About Tallinn 2.0 ... Whatever It Says." *Lawfare*, January 4, 2017. Accessed January 20, 2021. https://www.lawfareblog.com/warning-about-tallinn-20-...-whatever-it-says.

Alexander, David. "US Reserves Right to Meet Cyber Attack With Force." *Reuters*, November 15, 2011. Accessed February 10, 2021. https://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116.

Bing, Christopher, Jack Stubbs, Raphael Satter, and Joseph Menn. "Exclusive: Suspected Chinese Hackers Used SolarWinds Bug to Spy on 'US Payroll Agency—Sources." *Reuters*, February 2, 2021. Accessed February 5, 2021. https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8.

CBS Chicago. "Illinois Election Chief to Testify at Senate Panel on Russian Hacking," June 21, 2017. Accessed February 25, 2019. https://chicago.cbslocal.com/2017/06/21/illinois-state-board-of-elections-russian-hacking-senate-intelligence-committee/.

Chernenko, Elena. "Russia Warns Against NATO Document Legitimizing Cyberwars." *Russia Beyond*, May 29, 2013. Accessed January 25, 2021. https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html.

Clayton, Mark. "How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant." *Christian Science Monitor*, November 16, 2010. Accessed February 15, 2021. https://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

Cohen, Zachary, Vivian Salama, and Brian Fung. "US Officials Scramble to Deal With Suspected Russian Hack of Government Agencies." *CNN Politics*, December 14, 2020. Accessed February 6, 2021. https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia.

Corera, Gordon. "NHS Cyber-Attack Was 'Launched from North Korea'." *BBC News*, June 16, 2017. Accessed December 22, 2020. https://www.bbc.com/news/technology-40297493.

Corfield, Gareth. "SolarWinds Malware Was Sneaked Out of the Firm's Orion Build Environment 6 Months Before Anyone Realised It Was There—Report." *The Register*, January 12, 2021. Accessed January 18, 2021. https://www.theregister.com/2021/01/12/solarwinds_tech_analysis_crowdstrike/.

Corn, Gary. "Tallinn Manual 2.0—Advancing the Conversation." *Just Security*, February 15, 2017. Accessed January 25, 2021. https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

Davis, Austin. "Berlin Gold Coin Heist: 3 Sentenced to Jail." *DW*, February 20, 2020. Accessed June 11, 2020. https://www.dw.com/en/berlin-gold-coin-heist-3-sentenced-to-jail/a-52441680.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, August 21, 2007. Accessed January 14, 2021. https://www.wired.com/2007/08/ff-estonia.

Day, Chad, and Eric Tucker. "Court Records Reveal a Mueller Report Right in Plain View." *CTV News*, February 23, 2019. Accessed February 25, 2019. https://www.ctvnews.ca/world/court-records-reveal-a-mueller-report-right-in-plain-view-1.4309843.

Deeks, Ashley. "Tallinn 2.0 and a Chinese View on the Tallinn Process." *Lawfare*, May 31, 2015. Accessed January 25, 2021. https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.

Eichensehr, Kristen E. "International Agreements—and Disagreements—on Cybersecurity." *Just Security*, October 24, 2014. Accessed November 23, 2020. https://www.justsecurity.org/16706/international-agreements-and-disagreements-on-cybersecurity/.

Elliott, Jennifer, and Nigel Jenkinson. "Cyber Risk is the New Threat to Financial Security." *IMFBlog*, December 7, 2020. Accessed February 19, 2020. https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/.

Fung, Brian. "Why the US Government Hack Is Literally Keeping Security Experts Awake At Night." *CNN Business*, December 16, 2020. Accessed January 18, 2021. https://www.cnn.com/2020/12/16/tech/solarwinds-orion-hack-explained/index.html.

Garcia, Monique, and Patrick M. O'Connell. "Illinois Elections Board 'Very Likely' Named in Mueller Indictment of Russian Hackers, Officials Say." *Chicago Tribune*, July 13, 2018. Accessed February 25, 2019. https://www.chicagotribune.com/news/local/politics/ct-met-illinois-elections-board-russia-indictment-20180713-story.html.

Ghosh, Pallab. "First Ever Black Hole Image Released." *BBC News*, April 10, 2019. Accessed April 10, 2019. https://www.bbc.com/news/science-environment-47873592.

Goldstein, Joseph. "Doctors Without Borders Says Clues Point to 'Illegal' U.S. Strike on Afghan Hospital." *New York Times*, November 5, 2015. Accessed September 5, 2020. https://www.nytimes.com/2015/11/06/world/asia/doctors-without-borders-seeks-explanation-for-kunduz-hospital-attack.html.

Goldstein, Matthew. "Puerto Rico's Positive Business Slogans Can't Keep the Lights On." *New York Times*, March 5, 2018. Accessed February 28, 2019. https://www.nytimes.com/2018/03/05/business/puerto-rico-business-maria.html.

Graff, Garrett N. "The Man Who Speaks Softly—and Commands a Big Cyber Army." *Wired*, October 13, 2020. Accessed October 14, 2020. https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/.

Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway—with Me in It." *Wired*, July 21, 2015. Accessed January 11, 2018. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

———. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. Accessed February 4, 2021. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

———. "US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit." *Wired*, October 19, 2020. Accessed February 4, 2021. https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/.

Haxhiaj, Serbeze, and Filip Rudic. "Lost Property: Kosovo's Missing Records Prolong Post-War Legal Battles." *Balkan Insight*, April 3, 2019. Accessed May 12, 2019. https://balkaninsight.com/2019/04/03/lost-property-kosovos-missing-records-prolong-post-war-legal-battles/.

Heath, Nick. "How Estonia Became an E-Government Powerhouse." *Tech Republic*, February 19, 2019. Accessed January 15, 2021. https://www.techrepublic.com/article/how-estonia-became-an-e-government-powerhouse/.

Hughes, Owen. "WannaCry Impact on NHS Considerably Larger Than Previously Suggested." *Digital Health*, October 27, 2017. Accessed December 19, 2020. https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/.

Jordan, Bryant. "US Still Has No Definition for Cyber Acts of War." *Military.com*, June 22, 2016. Accessed January 18, 2021. https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html.

Kennedy, John. "Impact of WannaCry: MajorDisruption As Organisations Go Back to Work." *Silicon Republic*, May 15, 2017. Accessed December 19, 2020. https://www.siliconrepublic.com/enterprise/wannacry-impact-organisations-attack.

Kessler, Glenn. "The Iraq War and WMDs: An Intelligence Failure or White House Spin?" *Washington Post*, March 22, 2019. Accessed December 23, 2020. https://www.washingtonpost.com/politics/2019/03/22/iraq-war-wmds-an-intelligence-failure-or-white-house-spin/.

Kilovaty, Ido, and Itamar Mann. "Towards a Cyber-Security Treaty." *Just Security*, August 3, 2016. Accessed November 23, 2020. https://www.justsecurity.org/32268/cyber-security-treaty/.

Kleinwächter, Wolfgang. "International Law and Cyberspace: It's the 'How', Stupid." CircleID, December 10, 2020. Accessed January 20, 2021. http://www.circleid.com/posts/20201210-international-law-and-cyberspace-its-the-how-stupid/.

Leckie, Scott. "Resolving Kosovo's Housing Crisis: Challenges for the UN Housing and Property Directorate." *Forced Migration Review* 7 (April 2000): 12–15. Accessed May 15, 2019. https://www.fmreview.org/sites/fmr/files/FMRdownloads/en/land-and-property-issues/leckie.pdf.

Leetaru, Kalev. "Why Are We So Afraid of Petabytes?" *Forbes*, January 17, 2017. Accessed May 1, 2019. https://www.forbes.com/sites/kalevleetaru/2017/01/17/why-are-we-so-afraid-of-petabytes/#609365765875.

Marks, Joseph, and Tonya Riley. "The Cybersecurity 202: U.S. Voting Machines Vulnerable to Hacks in 2020, Researchers Find." *Washington Post*, September 27, 2019. Accessed October 6, 2020. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/09/27/the-cybersecurity-202-u-s-voting-machines-vulnerable-to-hacks-in-2020-researchers-find/5d8cf823602ff14beb3da99e/.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*, April 27, 2017. Accessed January 14, 2021. https://www.bbc.com/news/39655415.

Monahan, Kevin, Cynthia McFadden, and Didi Martinez. "'Online and Vulnerable': Experts Find Nearly Three Dozen U.S. Voting Machines Connected to Internet." *NBC News*, January 10, 2020. Accessed March 8, 2021. https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436.

Mracevich, Milorad. "Anti-Muslim Violence Rocks Serbia." *Balkan Reconstruction Report*, March 22, 2004. Accessed March 29, 2019. https://www.ceeol.com/search/article-detail?id=1171.

Murphy, Jessica. "Black Nova Scotians May Finally Get Title to Their Land." *BBC News*, October 8, 2017. Accessed May 22, 2019. https://www.bbc.com/news/world-us-canada-41488953.

Nakashima, Ellen. "Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes." *Washington Post*, January 12, 2018. Accessed February 4, 2021. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

———. "US Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *Washington Post*, February 27, 2019. Accessed February 4, 2021. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

Nakashima, Ellen, and Steven Mufson. "Hackers Have Attacked Foreign Utilities, CIA Analyst Says." *Washington Post*, January 19, 2008, A4.

Nakasone, Paul M., and Michael Sulmeyer. "How to Compete in Cyberspace: Cyber Command's New Approach." *Foreign Affairs*, August 25, 2020. Accessed October 14, 2020. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

NATO Cooperative Cyber Defence Centre of Excellence. "CCDCOE to Host the Tallinn Manual 3.0 Process," December 14, 2020. Accessed January 18, 2021. https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.

Newman, Lily May. "The Leaked NSA Spy Tool That Hacked the World." *Wired*, March 7, 2018. Accessed December 21, 2020. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

News Is My Business. "Puerto Rico Property Registry Now 100% Electronic." Edited by Michelle Kantrow-Vázquez, April 1, 2016. Accessed February 28, 2019. http://newsismybusiness.com/puerto-rico-property-registry-now-100-electronic/.

North Atlantic Treaty Organization (NATO). "Press Conference of the NATO Spokesman, Jamie Shea, and Air Commodore David Wilby." Transcript. March 31, 1999. Accessed March 25, 2019. https://www.nato.int/kosovo/press/p990331a.htm.

Norton Rose Fulbright. "WannaCry Ransomware Attack Summary." *Data Protecton Report*, May 17, 2017. Accessed December 21, 2020. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/.

Nova Scotia. *Government Helping Communities Get Clear Title to Land*. News release. African Nova Scotian Affairs, September 27, 2017. Accessed May 22, 2019. https://novascotia.ca/news/release/?id=20170927001.

Paul, Ryan. "Iranian Power Plant Infected by Stuxnet, Allegedly Undamaged." *Ars Technica*, September 27, 2010. Accessed November 23, 2020. https://arstechnica.com/information-technology/2010/09/iranian-power-plant-infected-by-stuxnet-allegedly-undamaged/.

Ponniah, Kevin, and Lazara Marinković. "The Night the US Bombed a Chinese Embassy." *BBC News*, May 7, 2019. Accessed May 7, 2019. https://www.bbc.com/news/world-europe-48134881.

Reuters. "DOE Chief Sees No Blackout Penalty for FirstEnergy," November 19, 2003. Accessed September 29, 2020. https://web.archive.org/web/20040224080845/http://www.forbes.com/markets/newswire/2003/11/19/rtr1153863.html.

Robles, Frances, and Jugal K. Patel. "On Hurricane Maria Anniversary, Puerto Rico Is Still in Ruins." *New York Times*, September 20, 2018. Accessed February 28, 2019. https://www.nytimes.com/interactive/2018/09/20/us/puerto-rico-hurricane-maria-housing.html.

Schmitt, Michael, and Liis Vihul. "International Cyberlaw Politicized: UN GGE's Failure to Advance Cyber Norms." *Just Security*, June 30, 2017. Accessed November 23, 2020. https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

Schmitt, Michael N., and Sean Fahey. "WannaCry and the International Law of Cyberspace." *Just Security*, December 22, 2017. Accessed December 19, 2020. https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/.

Sharwood, Simon. "SolarWinds Mess That Flared in the Holidays: Biz Confirms Malware Targeted Crocked Orion Product." *The Register*, January 4, 2021. Accessed January 18, 2021. https://www.theregister.com/2021/01/04/solarwinds_malware_confirmed/.

Sieff, Kevin. "U.S. Is Denying Passports to Americans Along the Border, Throwing Their Citizenship Into Question." *Washington Post*, September 13, 2018. Accessed March 8, 2019. https://www.washingtonpost.com/world/the_americas/us-is-denying-passports-to-americans-along-the-border-throwing-their-citizenship-into-question/2018/08/29/1d630e84-a0da-11e8-a3dd-2a1991f075d5_story.html?noredirect=on.

Snider, Mike. "Robert Mueller Investigation: What Is a Russian Troll Farm?" *USA Today*, February 16, 2018. Accessed October 7, 2020. https://www.usatoday.com/story/tech/news/2018/02/16/robert-mueller-investigation-what-russian-troll-farm/346159002/.

Tamkin, Emily. "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 2017. Accessed September 7, 2019. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

Tanner, Jari. "Violence Continues Over Estonia's Removal of Soviet War Statue." *Boston Globe*, April 28, 2007. Accessed January 14, 2021. http://archive.boston.com/news/world/asia/articles/2007/04/28/violence_continues_over_estonias_removal_of_soviet_war_statue/.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, May 17, 2007. Accessed September 10, 2020. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

Turak, Natasha. "Cyberattack and Proxy Violence Warnings As Iran Threatens 'Nightmare' Revenge against US." *CNBC*, January 7, 2020. Accessed May 24, 2020. https://www.cnbc.com/2020/01/07/how-iran-could-retaliate-against-the-us-after-solemani-killing.html.

United Kingdom Foreign & Commonwealth Office. "Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks." Press release, December 19, 2017. Accessed December 22, 2020. https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

United Nations. "Tackling State Responsibility, Diplomatic Protection Drafts, Sixth Committee Delegates Argue over Elaborating Texts into Conventions." Meetings coverage, Sixth Committee, Seventy-Fourth Session, 13th & 14th Meetings (AM & PM), GA/L/3598, October 15, 2019. Accessed December 11, 2020. https://www.un.org/press/en/2019/gal3598.doc.htm.

Weinberger, Sharon. "How Israel Spoofed Syria's Air Defence System." *Wired*, October 4, 2007. Accessed February 1, 2021. https://www.wired.com/2007/10/how-israel-spoo/.

Weingarten, Dwight. "International Cyber Laws Remain Work in Progress, DoD's Wingfield Says." *MeriTalk*, June 19, 2020. Accessed January 18, 2021. https://www.meritalk.com/articles/international-cyber-laws-remain-work-in-progress-dods-wingfield-says/.

Williams, Megan. "'Dignity itself': Saving World Heritage Sites from 'Cultural Cleansing' Won't Be Easy." *CBC News*, March 31, 2017. Accessed March 31, 2017. http://www.cbc.ca/news/world/saving-culture-g7-megan-williams-1.4048707.

Wolfe, Ian, and Brendan Pierson. "Explainer—US Government Hack: Espionage or Act of War?" *Reuters*, December 19, 2020. Accessed January 18, 2021. https://www.reuters.com/article/global-cyber-legal-idUSKBN28T0HH.

Zetter, Kim. "Stuxnet Missing Link Found, Resolves Some Mysteries Around the Cyberweapon." *Wired*, February 26, 2013. Accessed December 27, 2020. https://www.wired.com/2013/02/new-stuxnet-variant-found/.

Other documents

Aberdeen. *Petarack*. Product specification sheet. 2018. Accessed May 1, 2019. https://www.aberdeeninc.com/wwwinc/pdf/Petarack-One-Sheet.pdf.

Alex, Dan. "Friedrichshafen G.III Bomber/Night Bomber Aircraft." *Military Factory*, July 31, 2019. Accessed September 17, 2020. https://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=602.

Beck, Terry. "Mouse Trap Game in Slow Motion 19 Seconds." Video recording, April 27, 2015. Accessed May 7, 2020. https://www.youtube.com/watch?v=sy840XvnQRA.

Blue Shield. "Defining Cultural Heritage and Cultural Property," February 11, 2020. Accessed March 5, 2021. https://theblueshield.org/defining-cultural-heritage-and-cultural-property/.

———. "Who We Are," February 11, 2020. Accessed March 5, 2021. https://theblueshield.org/about-us/what-is-blue-shield/.

Bonner, Marianne. "Liability for Damage to Electronic Data." *The Balance Small Business*, December 8, 2018. Accessed October 16, 2020. https://www.thebalancesmb.com/liability-for-damage-to-electronic-data-462620.

Chimene-Weiss, Sara, Sol Eppel, Jeremy Feigenbaum, Seth Motel, Ingrid Pangandoyon, Michael D'Ortenzio, and Ross Cheit. "Understanding the Iran-Contra Affairs: Nicaragua and Iran Timeline." Brown University, 2010. Accessed May 24, 2020. https://www.brown.edu/Research/Understanding_the_Iran_Contra_Affair/timeline-n-i.php.

Cisco Systems. *2015 Annual Security Report*. Technical report. San Jose, CA: Cisco Systems, 2015. Accessed April 28, 2016. http://www.cisco.com/web/offers/pdfs/cisco-asr-2015.pdf.

———. *2018 Annual Security Report*. Technical report. San Jose, CA: Cisco Systems, 2018. Accessed March 2, 2021. https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf.

Coopee, Todd. "Mouse Trap by Ideal (1963)." *Toy Tales*, June 29, 2018. Accessed May 7, 2020. https://toytales.ca/mouse-trap-ideal-1963.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. *On Cyber Warfare*. Technical report. The Royal Institute of International Affairs, October 2010. http://kms2.isn.ethz.ch/serviceengine/Files/ESDP/124065/ipublicationdocument_singledocument/d922df2d-c90f-4fa6-978a-dc27940df964/en/17817_r1110_cyberwarfare.pdf.

Department of Defense [USA]. *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*. Technical report. November 2011. Accessed February 10, 2021. https://www.acqnotes.com/Attachments/DoD%20Cyberspace%20Policy%20Report%20A%20Report%20to%20Congress%20Pursuant%20to%20the%20NDA%20Act%20Nov2011.pdf.

Department of Homeland Security [USA]. *National Terrorism Advisory System Bulletin*, January 4, 2020. Accessed May 24, 2020. https://www.dhs.gov/sites/default/files/ntas/alerts/20_0104_ntas_bulletin.pdf.

Evstafiev, Mikhail. *Vedran Smailović, The Cellist of Sarajevo*. Photograph, 1992. Accessed March 18, 2021. https://en.wikipedia.org/wiki/Vedran_Smailovi%C4%87#/media/File:Evstafiev-bosnia-cello.jpg.

Georgieva, Kristalina. "Financial Inclusion and Cybersecurity in the Digital Age." International Monetary Fund (IMF). Speech delivered to (Virtual) Conference on Financial Inclusion and Cybersecurity, December 10, 2020. Accessed February 19, 2021. https://www.imf.org/en/News/Articles/2020/12/10/sp121020-financial-inclusion-and-cybersecurity-in-the-digital-age.

Harke, Patricia N. *Cyberspace: A Lawless World*. Research report. Maxwell Air Force Base, AL: Air Command and Staff College, Air University, 2016. Accessed January 20, 2021. https://apps.dtic.mil/sti/pdfs/AD1041050.pdf.

Imperva, Inc. "Incapsula Finds Malicious Bots Account for Approximately 30 Percent of Internet Traffic." Imperva, Inc., December 29, 2014. Accessed April 28, 2016. https://www.incapsula.com/about/press-releases/incapsula-finds-malicious-bots-account-for-approximately-30-percent-of-internet-traffic/.

International Committee of the Red Cross (ICRC). *Treaties, States Parties and Commentaries*, 2020. Accessed December 28, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/.

———. "Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 29 July 1899." *Treaties, States Parties and Commentaries*. Accessed January 1, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=CD0F6C83F96FB459C12563CD002D66A1&action=openDocument.

———. "Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, 6 July 1906." *Treaties, States Parties and Commentaries*. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=C64C3E521F5CC28FC12563CD002D6737&action=openDocument.

———. "Convention for the Amelioration of the Condition of the Wounded in Armies in the Field. Geneva, 22 August 1864." *Treaties, States Parties and Commentaries*. Accessed December 28, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=477CEA122D7B7B3DC12563CD002D6603&action=openDocument.

———. "Declaration Respecting Maritime Law, Paris, 16 April 1856." *Treaties, States Parties and Commentaries*. Accessed December 28, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=10207465E7477D90C12563CD002D65A3&action=openDocument.

———. "Historical Treaties and Documents: By Date." *Treaties, States Parties and Commentaries*. Accessed December 28, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesHistoricalByDate.xsp.

———. "ICRC, Disintegration of State Structures." *How Does Law Protect in War? Online Casebook*, 1998. Accessed December 15, 2020. https://casebook.icrc.org/case-study/icrc-disintegration-state-structures#part_ii_2.

———. "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts." In *31st International Conference of the Red Cross and Red Crescent*. doc. 31IC/11/5.1.2. Report. Geneva, CH: International Committee of the Red Cross, November 28–December 1, 2011. Accessed November 27, 2020.

International Committee of the Red Cross (ICRC). "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts." In *32nd International Conference of the Red Cross and Red Crescent*. doc. 32IC/15/11. Report. Geneva, CH: International Committee of the Red Cross, December 8–10, 2015. Accessed March 6, 2021. https://rcrcconference.org/app//uploads/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf.

———. "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts." In *33rd International Conference of the Red Cross and Red Crescent*. doc. 33IC/19/9.7. Report. Geneva, CH: International Committee of the Red Cross, December 9–13, 2019. Accessed November 28, 2020. https://shop.icrc.org/download/ebook?sku=4427/002-ebook.

———. "Manual of the Laws of Naval War, Oxford, 9 August 1913." *Treaties, States Parties and Commentaries*. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=0F63D17A90E5CDC0C12563CD002D68EF&action=openDocument.

———. "Principles of International Law Recognized in the Charter of the Nüremberg Tribunal and in the Judgment of the Tribunal, 1950." *Treaties, States Parties and Commentaries*. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=854DDAACFDE285E4C12563CD002D6B95&action=openDocument.

———. "Project of an International Declaration Concerning the Laws and Customs of War, Brussels, 27 August 1874." *Treaties, States Parties and Commentaries*. Accessed January 1, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=42F78058BABF9C51C12563CD002D6659&action=openDocument.

International Institute of Humanitarian Law. San Remo Manual on International Law Applicable to Armed Conflicts at Sea, June 12, 1994. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/5B310CC97F166BE3C12563F6005E3E09/FULLTEXT/IHL-89-EN.pdf.

Internet Corporation for Assigned Names and Numbers (ICANN). "Articles of Incorporation," November 21, 1998. Accessed January 20, 2021. https://www.icann.org/resources/pages/articles-2012-02-25-en.

Legal Information Institute. "Black letter law." *Wex*. Accessed December 31, 2020. https://www.law.cornell.edu/wex/black_letter_law.

———. "*Opinio juris* (international law)." *Wex*. Accessed January 28, 2021. https://www.law.cornell.edu/wex/opinio_juris_(international_law).

Lemkin, Raphael. "Genocide as a Crime under International Law." American Jewish History Society, manuscript collection P-154, Raphael Lemkin collection, box 6, folder 2, 1948–51. Accessed February 21, 2019. http://digital.cjh.org:80/R/-?func=dbin-jump-full&object_id=398972&silo_library=GEN01.

Library and Archives Canada. "Legal Deposit," February 22, 2018. Accessed April 19, 2018. https://www.bac-lac.gc.ca/eng/services/legal-deposit/Pages/legal-deposit.aspx.

Microsoft Corporation. "Diplomatic Immunity for Data: Estonia Creates a Virtual Embassy." *Microsoft EU Policy Blog*, December 14, 2017. Accessed March 7, 2021. https://blogs.microsoft.com/eupolicy/2017/12/14/diplomatic-immunity-data-estonia-creates-virtual-embassy/.

———. "Fixed Lifecycle Policy," April 13, 2010. Accessed December 21, 2020. https://docs.microsoft.com/en-us/lifecycle/policies/fixed.

———. "Support for Windows XP Ended," May 3, 2018. Accessed December 21, 2020. https://www.microsoft.com/en-ca/microsoft-365/windows/end-of-windows-xp-support.

NATO Cooperative Cyber Defence Centre of Excellence. "About Us," August 17, 2020. Accessed January 19, 2021. https://ccdcoe.org/about-us/.

North Atlantic Treaty Organization (NATO). "Centres of Excellence," November 3, 2020. Accessed January 19, 2021. https://www.nato.int/cps/en/natolive/topics_68372.htm.

Nova Scotia. *Land Titles Clarification Act*. RSNS c. 250, s. 1. Formerly the *Community Land Titles Act*, SNS 1964, c. 3. 1964. Accessed May 22, 2019. https://nslegislature.ca/sites/default/files/legc/statutes/landtitl.htm.

Nova Scotia Archives. "African Nova Scotians in the Age of Slavery and Abolition: Black Loyalists, 1783–1792," May 2019. Accessed May 22, 2019. https://novascotia.ca/archives/Africanns/results.asp?Search=&SearchList1=2&Language=English.

———. "African Nova Scotians in the Age of Slavery and Abolition: Establishment of the Negroes in Nova Scotia, Appendix 23." Transcription of portion of Minutes of Council, March 11, 1841. May 2019. Accessed May 22, 2019. https://novascotia.ca/archives/africanns/archives.asp?ID=137&Transcript=1.

Office of the Director of National Intelligence [USA]. *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence community assessment, ICA 2017-01D, January 6, 2017. Accessed February 5, 2021. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Ontario. "Ontario Onwards: Action Plan," November 30, 2020. Accessed March 18, 2021. https://www.ontario.ca/page/ontario-onwards-action-plan#section-3.

Ontario Council of University Libraries (OCUL). "Cancellation of the Mandatory Long-Form Census—Background and Impact," January 5, 2015. Accessed March 4, 2021. https://ocul.on.ca/node/3400.

Organization for Security and Co-operation in Europe (OSCE) Mission in Kosovo. *An Assessment of the Voluntary Returns Process in Kosovo*. Returns and repatriation report. Organization for Security and Co-operation in Europe, October 2012. Accessed May 12, 2019. https://www.osce.org/kosovo/96805?download=true.

———. *An Assessment of the Voluntary Returns Process in Kosovo*. Returns and repatriation report. Organization for Security and Co-operation in Europe, October 2014. Accessed May 16, 2019. https://www.osce.org/kosovo/129321?download=true.

———. *Challenges in the Resolution of Conflict-Related Property Claims in Kosovo*. Returns and repatriation report. Organization for Security and Co-operation in Europe, June 2011. Accessed May 12, 2019. https://www.osce.org/kosovo/80435?download=true.

Riedlmayer, András J. "Libraries and Archives in Kosova: A Postwar Report." *Bosnia Report*, nos. 13/14 (December 1999–February 2000). Accessed March 21, 2019. http://www.bosnia.org.uk/bosrep/decfeb00/libraries.cfm.

robotstxt.org. "About */robots.txt*," 2007. Accessed May 12, 2019. http://www.robotstxt.org/robotstxt.html.

Sandvine Incorporated ULC. *2016 Global Internet Phenomena: Spotlight: Encrypted Internet Traffic*. Technical report. Waterloo, ON: Sandvine Incorporated ULC, February 2016. Accessed April 28, 2016. https://www.sandvine.com/downloads/general/global-internet-phenomena/2016/global-internet-phenomena-spotlight-encrypted-internet-traffic.pdf.

Simmonds, Angela. *This Land Is Our Land: African Nova Scotian Voices from the Preston Area Speak Up*. Project report. Schulich School of Law, Dalhousie University, August 19, 2014. Accessed May 22, 2019. https://nsbs.org/sites/default/files/ftp/EQ20140819_ThisLandIsOurLand_Final.pdf.

SolarWinds Corporation. United States Security and Exchange Commission Form 8-K, December 17, 2020. Accessed January 18, 2021. https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/6dd04fe2-7d10-4632-89f1-eb8f932f6e94.pdf.

Statistics Estonia. "RV0222U: Population, 1 January by Year, Sex, County and Ethnic Nationality," January 1, 2020. Accessed January 15, 2021. https://andmed.stat.ee/en/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV0222U/table/tableViewLayout1.

Symanovich, Steve. "What Is a Honeypot? How It Can Lure Cyberattackers." NortonLifeLock, May 26, 2020. Accessed February 5, 2021. https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html.

Tison, Annette. "Anatomy Of a Bombing Mission." *392nd Bomb Group*, 2017. Accessed October 1, 2020. https://www.b24.net/MissionAnatomy.htm.

U.S. Department of State Country Report on Human Rights Practices 2002 — Yugoslavia, Federal Republic of. United States Department of State, March 31, 2003. Accessed March 28, 2018. http://www.refworld.org/docid/3e918c46c.html.

U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Causal analysis. April 2004. Accessed September 29, 2020. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

United Nations. Final Act of the International Conference on Human Rights, Teheran, April 22–May 13, 1968, A/CONF.32/41. Accessed February 11, 2021. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N68/958/82/PDF/N6895882.pdf?OpenElement.

———. "What We Do," December 18, 2018. Accessed October 2, 2019. https://www.un.org/en/sections/what-we-do/.

United Nations General Assembly. Report of the Working Group of Experts on People of African Descent on Its Mission to Canada, August 16, 2017. Report, A/HRC/36/60/Add.1. Human Rights Council. Accessed May 22, 2019. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/239/60/PDF/G1723960.pdf?OpenElement.

———. Status of the Protocols Additional to the Geneva Conventions of 1949 and Relating to the Protection of Victims of Armed Conflicts, September 12, 1990. Report of the Secretary-General, A/45/454. Accessed March 6, 2021. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N90/222/30/img/N9022230.pdf?OpenElement.

———. Status of the Protocols Additional to the Geneva Conventions of 1949 and Relating to the Protection of Victims of Armed Conflicts, August 26, 1998. Report of the Secretary-General, A/53/287. Accessed March 6, 2021. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/249/43/pdf/N9824943.pdf?OpenElement.

United Nations High Commissioner for Refugees (UNHCR). *Birth Registration*. Child Protection Issue Brief. Geneva, CH, August 2013. Accessed April 11, 2019. https://www.refworld.org/docid/523fe9214.html.

United Nations International Law Commission. Principles of International Law Recognized in the Charter of the Nüremberg Tribunal and in the Judgment of the Tribunal, July 29, 1950. Accessed January 3, 2021. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/854DDAACFDE285E4C12563CD002D6B95/FULLTEXT/IHL-58-EN.pdf.

United States Central Command. *Investigation Report of the Airstrike on the Médecins Sans Frontières / Doctors Without Borders Trauma Center in Kunduz, Afghanistan on 3 October 2015*. Investigation report and summary. November 25, 2015. Accessed September 5, 2020. https://web.archive.org/web/20190331041350/https://info.publicintelligence.net/CENTCOM-KunduzHospitalAttack.pdf.

United States President. *Critical Infrastructure Protection*. Presidential Decision Directive/NSC 63. May 22, 1998. Accessed August 15, 2016. https://fas.org/irp/offdocs/pdd/pdd-63.pdf.

Valenta, Jiri, and Leni Friedman Valenta. *Russia's Strategic Advantage in the Baltics: A Challenge to NATO?* Mideast Security and Policy Studies 143. Report. Ramat Gan, IL: The Begin-Sadat Center for Strategic Studies, Bar-Ilan University, January 2018. Accessed January 19, 2021. https://www.jstor.org/stable/resrep16828.

Appendices

Appendix A

Selected milestones in international law

While every treaty, declaration, judgement, or manual is important to international law, they are not of equal significance in the development, codification, or promulgation of international law. This appendix identifies the documents that demonstrate the evolution of international law to the point where its application to cyberwarfare could be codified in the *Tallinn Manual*. The documents are listed in chronological order with a brief statement of their significance and the aspects of international law that they develop.

A.1 Between the Crimean and First World Wars (1856–1914)

Paris Declaration, 1856

- Identifies desire "to establish a uniform doctrine" with respect to maritime law[1]
- Model for accession to treaties by non-signatory states[2]
- *Jus in bello*: clarifies neutrality and blockades; bans privateering[3]

[1]Declaration Respecting Maritime Law, Paris, April 16, 1856, preamble, accessed December 28, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/10207465E7477D90C12563CD002D65A3/FULLTEXT/IHL-1-EN.pdf (hereafter cited as Paris Declaration).

[2]Department of Defense [USA], *Department of Defense Law of War Manual*, §19.4.

[3]Paris Declaration, Art.1–4.

- In force for still-extant states parties and their successor states[4]

Lieber Code, 1863

- *Jus in bello*: prohibits poison, unnecessary suffering, rape, murder, and other violent or criminal acts[5]
- Humanitarian rules: provides for prisoners of war[6] and recognition (but little protection) for noncombatants[7]
- Cultural objects: provides limited protection for hospitals, institutes of religion, charity, education, and arts and sciences[8]
- Some aspects still in force for American armed forces[9]

Geneva Convention, 1864

- *Jus in bello*: establishes neutrality of hospitals, ambulances, and their personnel;[10] specifies use of a red cross as distinctive marking for humanitarian personnel, facilities, and objects[11]
- Humanitarian rules: provision of care for wounded combatants[12]
- Superseded by later conventions[13]

---

[4] International Committee of the Red Cross (ICRC), "Declaration Respecting Maritime Law, Paris, 16 April 1856."

[5] United States of America, "Instructions for the Government of Armies of the United States in the Field (Lieber Code)," April 24, 1863, Art. 44, 47, 70, 71, accessed December 28, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/A25AA5871A04919BC12563CD002D65C5/FULLTEXT/IHL-L-Code-EN.pdf (hereafter cited as Lieber Code).

[6] Lieber Code, §§3, 6, 7.

[7] Lieber Code, Art. 18, 19.

[8] Lieber Code, Art. 34–36, 118.

[9] Department of Defense [USA], *Department of Defense Law of War Manual*, §19.3.

[10] International Committee of the Red Cross (ICRC), Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Geneva, August 22, 1864, Art. 1, 2, accessed December 28, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/477CEA122D7B7B3DC12563CD002D6603/FULLTEXT/IHL-GC1864-EN.pdf (hereafter cited as Geneva Convention (1864)).

[11] Geneva Convention (1864), Art. 7.

[12] Geneva Convention (1864), Art. 5, 6.

[13] International Committee of the Red Cross (ICRC), "Convention for the Amelioration of the Condition of the Wounded in Armies in the Field. Geneva, 22 August 1864," *Treaties,*

St. Petersburg Declaration, 1868

- *Jus in bello*: first prohibition of certain weapons;[14] "[t]he only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy"[15] (proportionality)
- Anticipates need for further propositions "in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which [the states parties] have established, and to conciliate the necessities of war with the laws of humanity"[16]
- In force for still-extant states parties and their successor states[17]

Brussels Declaration, 1874

- *Jus in bello*: rules for occupying powers;[18] classification of belligerents;[19] forbidding certain "means of injuring the enemy";[20] denying rights as a combatant to those caught in hostile territory while con-

---

States Parties and Commentaries, accessed December 28, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=477CEA122D7B7B3DC12563CD002D6603&action=openDocument.

[14] International Committee of the Red Cross (ICRC), "Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, 29 November / 11 December 1868," *Treaties, States Parties and Commentaries*, accessed December 31, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=3C02BAF088A50F61C12563CD002D663B&action=openDocument.

[15] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, December 11, 1868, accessed December 31, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/3C02BAF088A50F61C12563CD002D663B/FULLTEXT/IHL-6-EN.pdf (hereafter cited as St. Petersburg Declaration).

[16] St. Petersburg Declaration.

[17] International Committee of the Red Cross (ICRC), "Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. Saint Petersburg, 29 November / 11 December 1868."

[18] Project of an International Declaration Concerning the Laws and Customs of War, Brussels, August 27, 1874, unratified, Art. 1–8, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/42F78058BABF9C51C12563CD002D6659/FULLTEXT/IHL-7-EN.pdf (hereafter cited as Brussels Declaration (1874)).

[19] Brussels Declaration (1874), Art. 9–11.

[20] Brussels Declaration (1874), Art. 12, 13.

ducting espionage[21]
- Humanitarian rules: provisions for prisoners of war;[22] care for sick and wounded according to the Geneva Convention (1864);[23] protection for hospitals from attack[24]
- Cultural objects: requires attackers to take "all necessary steps . . . to spare, as far as possible, buildings dedicated to art, science, or charitable purposes, . . . provided that they are not at that time being used for military purposes";[25] advocates legal settlement for "seizure, or destruction of, or wilful damage to institutions of [religion, charity, education, and the arts and sciences], historic monuments, works of art and science"[26]
- Never ratified[27]

Oxford Manual (Laws of War on Land), 1880

- Codification: first " 'Manual' suitable as a basis for national legislation in each State"[28]
- Informed by Brussels Declaration (1874)[29]
- Not treaty law, but an expression of "the accepted ideas of our age so far as this has appeared allowable and practicable"[30]

---

[21] Brussels Declaration (1874), Art. 19–21.

[22] Brussels Declaration (1874), Art. 23–34.

[23] Brussels Declaration (1874), Art. 35, 56.

[24] Brussels Declaration (1874), Art. 17.

[25] Brussels Declaration (1874), Art. 17.

[26] Brussels Declaration (1874), Art. 8.

[27] International Committee of the Red Cross (ICRC), "Project of an International Declaration Concerning the Laws and Customs of War, Brussels, 27 August 1874," *Treaties, States Parties and Commentaries*, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=42F78058BABF9C51C12563CD002D6659&action=openDocument.

[28] Institute of International Law (IIL), The Laws of War On Land, September 9, 1880, preamble, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/40371257507EBB71C12563CD002D6676/FULLTEXT/IHL-8-EN.pdf (hereafter cited as *Oxford Manual* (1880)).

[29] International Committee of the Red Cross (ICRC), "Project of an International Declaration Concerning the Laws and Customs of War, Brussels, 27 August 1874."

[30] *Oxford Manual* (1880), preamble.

- *Jus in bello*: Martens Clause on general protections where the laws of armed combat have not been codified;[31] separate declarations prohibiting use of gas weapons[32] and expanding (Dum-Dum) bullets[33]
- Humanitarian rules: incorporates Geneva Convention (1864) and future amendments[34] and adapts it to maritime war[35]
- Brussels Declaration (1874) served as foundation[36]

---

[31]"Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience." Hague Peace Conferences, Convention (II) with Respect to the Laws and Customs of War on Land, The Hague, July 29, 1899, preamble, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/CD0F6C83F96FB459C12563CD002D66A1/FULLTEXT/IHL-10-EN.pdf (hereafter cited as HC II (1899)).

[32]Hague Peace Conferences, Declaration (IV,2) Concerning Asphyxiating Gases, The Hague, July 29, 1899, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/B0625F804A9B2A64C12563CD002D66FF/FULLTEXT/IHL-13-EN.pdf (hereafter cited as HD IV.2 (1899)).

[33]Hague Peace Conferences, Declaration (IV,3) Concerning Expanding Bullets, The Hague, July 29, 1899, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/D528A73B322398B5C12563CD002D6716/FULLTEXT/IHL-14-EN.pdf (hereafter cited as HD IV.3 (1899)).

[34]Hague Peace Conferences, Convention (II) Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, July 29, 1899, Art. 22, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/CD0F6C83F96FB459C12563CD002D66A1/FULLTEXT/IHL-10-EN.pdf (hereafter cited as HC II (1899) Annex).

[35]Hague Peace Conferences, Convention (III) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention of 22 August 1864, The Hague, accessed January 3, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2B134D111958C73AC12563CD002D66C8/FULLTEXT/IHL-11-EN.pdf (hereafter cited as HC III (1899)).

[36]International Committee of the Red Cross (ICRC), "Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 29 July 1899," *Treaties, States Parties and Commentaries*, accessed January 1, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.

- HC II (1899), HD IV.2 (1899), and HD IV.3 (1899) still in force for still-extant states parties and their successor states not ratifying 1907 revisions[37]

Geneva Convention, 1906

- *Jus in bello* and anticipating *jus post bellum*: requirement for governments to "repress . . . as well as punish" persons who violate the Convention[38]
- Superseded by later conventions[39]

Hague Conventions and Declaration, 1907

- *Jus ad bellum*: requirement to give notice of a declaration of war to enemy and neutral states[40]
- *Jus in bello*: reaffirms Martens Clause of HC II (1899);[41] codification of

xsp?documentId=CD0F6C83F96FB459C12563CD002D66A1&action=openDocument.

[37] International Committee of the Red Cross (ICRC), "Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 29 July 1899."

[38] International Committee of the Red Cross (ICRC), Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, July 6, 1906, Art. 28, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/C64C3E521F5CC28FC12563CD002D6737/FULLTEXT/IHL-GC-1906-EN.pdf (hereafter cited as Geneva Convention (1906)).

[39] International Committee of the Red Cross (ICRC), "Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, 6 July 1906," *Treaties, States Parties and Commentaries*, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=C64C3E521F5CC28FC12563CD002D6737&action=openDocument.

[40] Hague Peace Conferences, Convention (III) Relative to the Opening of Hostilities, The Hague, October 18, 1907, Art. 1, 2, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/BD56907463617993C12563CD002D6774/FULLTEXT/IHL-18-EN.pdf (hereafter cited as HC III (1907)).

[41] Hague Peace Conferences, Convention (IV) Respectting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, October 18, 1907, preamble, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/4D47F92DF3966A7EC12563CD002D6788/FULLTEXT/IHL-19-EN.pdf (hereafter cited as HC IV (1907)).

laws of neutrality[42] and extension to naval war;[43] rules on underwater mines and torpedoes;[44] naval bombardment of undefended sites constrained in ways analogous to land-based bombardment[45]

- *Jus post bellum*: compensation for violations of the convention[46]
- Humanitarian rules: adaptation of Geneva Convention (1906) to maritime context[47]
- Human rights: belligerents cannot suspend rights of "nationals of the hostile party";[48] "family honour and rights, the lives of persons, and private property, as well as religious convictions and practice" are protected in occupied territory[49]
- Some protection for submarine cables in occupied territory[50]
- Many provisions still in force

---

[42]Hague Peace Conferences, Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, October 18, 1907, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/71929FBD2655E558C12563CD002D67AE/FULLTEXT/IHL-20-EN.pdf (hereafter cited as HC V (1907)).

[43]Hague Peace Conferences, Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, The Hague, October 18, 1907, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/06A47A50FE7412AFC12563CD002D6877/FULLTEXT/IHL-28-EN.pdf (hereafter cited as HC XIII (1907)).

[44]Hague Peace Conferences, Convention (VIII) Relative to the Laying of Automatic Submarine Contact Mines, The Hague, October 18, 1907, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/7D389CA23C22337BC12563CD002D67FF/FULLTEXT/IHL-23-EN.pdf (hereafter cited as H VIII (1907)).

[45]Hague Peace Conferences, Convention (IX) Concerning Bombardment by Naval Forces in Time of War, The Hague, October 18, 1907, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/F13F9FFC628FC33BC12563CD002D6819/FULLTEXT/IHL-24-EN.pdf (hereafter cited as HC IX (1907)); *cf.* HC IV (1907), Annex, Art. 25.

[46]HC IV (1907), Art. 3.

[47]Hague Peace Conferences, Convention (X) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention, The Hague, October 18, 1907, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/E5397A0FB560D0A9C12563CD002D6832/FULLTEXT/IHL-25-EN.pdf (hereafter cited as HC X (1907)).

[48]HC IV (1907), Annex, Art. 23(h).

[49]HC IV (1907), Annex, Art. 46.

[50]HC IV (1907), Annex, Art. 54.

Oxford Manual (Laws of Naval Warfare), 1913

- Codification of laws of naval warfare in the same vein as *Oxford Manual* (1880)
- Clarifies that mail is not subject to seizure (blockades notwithstanding)[51]
- Intended to be discussed at a future Hague Peace Conference[52]
- Not treaty law

A.2 Between the First and Second World Wars (1918–1939)

Geneva Gas and Bacteriological Weapons Protocol, 1925

- *Jus in bello*: declares use of gas as a means of war as a violation of international law, and extends prohibition to biological weapons[53]
- Still in force

[51] Instittute of International Law (IIL), Manual of the Laws of Naval War, August 9, 1913, Art. 53, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/0F63D17A90E5CDC0C12563CD002D68EF/FULLTEXT/IHL-33-EN.pdf (hereafter cited as *Oxford Manual* (1913)).

[52] International Committee of the Red Cross (ICRC), "Manual of the Laws of Naval War, Oxford, 9 August 1913," *Treaties, States Parties and Commentaries*, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=0F63D17A90E5CDC0C12563CD002D68EF&action=openDocument.

[53] Conference for the Supervision of the International Trade in Arms and Ammunition, Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, Geneva, June 17, 1925, preamble, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/921B4414B13E58B8C12563CD002D693B/FULLTEXT/IHL-36-EN.pdf (hereafter cited as Geneva Gas Protocol).

Geneva Conventions, 1929

- Humanitarian rules: protection for medical aircraft;[54] extensive detailing of rules concerning prisoners of war,[55] including prohibition of reprisals and collective punishment[56]
- Superseded by later conventions

London Treaty, Article 22, 1930

- *Jus in bello:* Submarines must also respect rules of maritime war concerning merchant ships[57]
- Still in force

Roerich Pact, 1935

- Cultural objects: protections for "treasures of culture": "historic monuments, museums, scientific, artistic, educational and cultural institutions" and their personnel, "in times of peace as well as war"[58]

[54] International Committee of the Red Cross (ICRC), Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field, Geneva, July 27, 1929, Art. 18, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/09DFB7A98E19533AC12563CD002D6997/FULLTEXT/IHL-GC-1929-1-EN.pdf (hereafter cited as Geneva Convention (Wounded and Sick, 1929)).

[55] International Committee of the Red Cross (ICRC), Convention Relative to the Treatment of Prisoners of War, Geneva, July 27, 1929, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/0BDEDDD046FDEBA9C12563CD002D69B1/FULLTEXT/IHL-GC-1929-2-EN.pdf (hereafter cited as Geneva Convention (Prisoners of War, 1929)).

[56] Geneva Convention (Prisoners of War, 1929), Art. 2, 11, 46.

[57] Treaty for the Limitation and Reduction of Naval Armaments, (Part IV, Art. 22, relating to submarine warfare), London, April 22, 1930, accessed January 4, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/32C5DA6C8C43775AC12563CD002D69CC/FULLTEXT/IHL-41-EN.pdf (hereafter cited as London Treaty (Art. 22)).

[58] Pan-American Union, Treaty on the Protection of Artistic and Scientific Institutions and Historic Monuments (Roerich Pact), Washington, 15 April 1935, April 15, 1935, preamble, Art. 1, accessed January 3, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/EE57F295093E44A4C12563CD002D6A3F/FULLTEXT/IHL-44-EN.pdf (hereafter cited as Roerich Pact).

- Still in force for states parties, supplemented by Cultural Property Convention

A.3 After the Second World War (1945–2021)

London Agreement and Charter of the International Military Tribunal, 1945

- *Jus post bellum*: established prosecution and punishment for crimes committed by European Axis in the course of the Second World War,[59] with crimes categorized as "crimes against peace," "war crimes," and "crimes against humanity"[60]
- Foundational for subsequent *ad hoc* tribunals and International Criminal Court[61]

United Nations Charter, 1945

- *Jus ad bellum*: United Nations Security Council has the power to authorize any use of military force;[62] states have right to act in self-defence "if an armed attack occurs"[63]
- Human rights: promotes "equal rights and self-determination of peoples"[64]
- Still in force

[59]Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal, London, August 8, 1945, Charter, Art. 1, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/87B0BB4A50A64DEAC12563CD002D6AAE/FULLTEXT/IHL-49-EN.pdf (hereafter cited as War Criminals Agreement).

[60]War Criminals Agreement, Charter, Art. 6.

[61]J. Holmes Armstead Jr., "The International Criminal Court: History, Development and Status," *Santa Clara Law Review* 38, no. 3 (January 1998): 748–9, accessed January 7, 2021, http://digitalcommons.law.scu.edu/lawreview/vol38/iss3/3.

[62]United Nations, Charter of the United Nations, October 24, 1945, 1 UNTS XVI, Art. 42, accessed October 6, 2015, http://www.refworld.org/docid/3ae6b3930.html (hereafter cited as UN Charter).

[63]UN Charter, Art. 51.

[64]UN Charter, Art. 55.

Convention on Genocide, 1948

- *Jus in bello*: establishes a definition of genocide,[65] identifies it as a "crime under international law,"[66] and requires a punishment for individuals found to have engaged in or encouraged genocide[67]
- Still in force

Universal Declaration of Human Rights, 1948

- Human rights:
  - rights to: "life, liberty, and the security of the person,"[68] a nationality and to change it,[69] equality before the law and right to equal protection under it,[70] due process in criminal proceedings,[71] own property,[72] participate in government and its selection,[73] access public services and social security,[74] safe work with equitable pay,[75] rest and leisure,[76] a minimally decent standard of living,[77] free elementary education,[78] "a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized"[79]

[65] United Nations General Assembly, Convention on the Prevention and Punishment of the Crime of Genocide, December 9, 1948, 78 UNTS 277, Art. 2, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/1507EE9200C58C5EC12563F6005FB3E5/FULLTEXT/IHL-51-EN.pdf (hereafter cited as Genocide Convention).

[66] Genocide Convention, Art. 1.

[67] Genocide Convention, Art. 3, 4.

[68] United Nations General Assembly, Universal Declaration of Human Rights, December 10, 1948, A/RES/217(III), Art. 3, accessed January 5, 2021, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf (hereafter cited as Universal Declaration).

[69] Universal Declaration, Art. 15.

[70] Universal Declaration, Art. 7.

[71] Universal Declaration, Art. 10–11.

[72] Universal Declaration, Art. 17.

[73] Universal Declaration, Art. 21.

[74] Universal Declaration, Art. 21, 22.

[75] Universal Declaration, Art. 23.

[76] Universal Declaration, Art. 24.

[77] Universal Declaration, Art. 25.

[78] Universal Declaration, Art. 26.

[79] Universal Declaration, Art. 28.

  - freedom of: movement within their state and the right to return to it,[80] "thought, conscience and religion,"[81] "opinion and expression,"[82] "peaceful assembly and association,"[83] participation in cultural activities[84]
  - freedom from: slavery in any form,[85] "torture or . . . cruel, inhuman or degrading treatment,"[86] "arbitrary interference with his privacy, family, home or correspondence [and] attacks upon his honour and reputation"[87]
  - duties to: recognize and respect "the rights and freedoms of others," "meet[] the just requirements of morality, public order, and the general welfare in a democratic society"[88]

- Not international law by itself, but foundational to the subsequent development of international law concerning human rights

Geneva Conventions, 1949

- *Jus in bello*: distinction between civilians of an enemy state in territory controlled by a belligerent state and the civilian population in general;[89] declaration and recognition of safe zones for the wounded and

[80] Universal Declaration, Art. 13.

[81] Universal Declaration, Art. 18.

[82] Universal Declaration, Art. 19.

[83] Universal Declaration, Art. 20.

[84] Universal Declaration, Art. 27, with the observation that both the arts and the sciences are part of cultural activity and development.

[85] Universal Declaration, Art. 4.

[86] Universal Declaration, Art. 5.

[87] Universal Declaration, Art. 12.

[88] Universal Declaration, Art. 29.

[89] International Committee of the Red Cross (ICRC), Convention (IV) Relative to the Protection of Civilian Persons in Time of War. Geneva, August 12, 1949, 75 UNTS 287, Art. 4, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/AE2D398352C5B028C12563CD002D6B5C/FULLTEXT/ATTXSYRB.pdf (hereafter cited as GC IV); Oscar M. Uhler et al., *Commentary: IV Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, ed. Jean S. Pictet, trans. Ronald Griffin and C. W. Dumbleton, vol. 4, The Geneva Conventions of 12 August 1949 (Geneva, CH: International Committee of the Red Cross (ICRC), 1958), 45, accessed January 8, 2021, https://b-ok.org/book/1266129/0a8d8d.

civilian population;[90] identification and protection of civilian hospitals and medical staff;[91] prohibition of "[r]eprisals against the wounded, sick, personnel, buildings or equipment protected by the Convention;"[92] no means for states to absolve themselves or other states of liability for grave breaches of the Conventions[93]

- *Jus post bellum*: formal inquiries into breaches of the Conventions if requested by any party to the conflict[94]
- Humanitarian rules: rules of basic care and protections apply to parties in non-international armed conflicts;[95] conventions apply to neutral states hosting or finding members of other states' armed forces in their territory;[96] protected persons shall not be subject to torture or experimentation[97]
- Human rights: occupying states have responsibility "to maintain the orderly government of the territory" while maintaining (as far as possible) the penal laws of the territory they occupy;[98] civilian persons in

[90] GC IV, Art. 15.

[91] GC IV, Art. 14, 18, 20.

[92] International Committee of the Red Cross (ICRC), Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, August 12, 1949, 75 UNTS 31, Art. 46, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/4825657B0C7E6BF0C12563CD002D6B0B/FULLTEXT/GC-I-EN.pdf (hereafter cited as GC I); International Committee of the Red Cross (ICRC), Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva, August 12, 1949, 75 UNTS 85, Art. 47, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2F5AA9B07AB61934C12563CD002D6B25/FULLTEXT/GC-II-EN.pdf (hereafter cited as GC II).

[93] GC I, Art. 51; GC II, Art. 52; GC IV, Art. 148.

[94] GC I, Art. 52; GC II, Art 53; GC IV, Art. 149.

[95] International Committee of the Red Cross (ICRC), Geneva Conventions I–IV, August 12, 1949, Common Art. 3 (hereafter cited as GC I–IV (1949)).

[96] GC I, Art. 4; GC II, Art. 5.

[97] GC I, Art. 12; GC II, Art. 12; International Committee of the Red Cross (ICRC), Convention (III) Relative to the Treatment of Prisoners of War, Geneva, August 12, 1949, 75 UNTS 135, Art. 13, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/77CB9983BE01D004C12563CD002D6B3E/FULLTEXT/GC-III-EN.002.pdf (hereafter cited as GC III).

[98] GC IV, Art. 64.

occupied territories have the right to due process in penal matters;[99] civilian enemy nationals retain certain rights and may not be unduly barred from leaving the country or occupied territory;[100] forcible relocation (not evacuation) from occupied territory prohibited;[101] no punishment for caring for the sick or wounded;[102] protections and provision for interned civilians set out in ways analogous to those for prisoners of war;[103] provisions for safety and education of orphaned children[104]

- GC II replaces HC X (1907)[105]
- Still in force

Recognition of Principles of International Law, 1950

- *Jus in bello, jus post bellum*: formalization of already-accepted principles set down in War Criminals Agreement[106] that "crimes against peace," "war crimes," and "crimes against humanity" are "punishable under international law";[107] no immunity from prosecution for heads of state or persons following orders[108]

[99] GC IV, Art. 65–75.

[100] GC IV, Art. 35–40, 47–48.

[101] GC IV, Art. 49.

[102] GC I, Art. 18.

[103] GC IV, Art. 79–135.

[104] GC IV, Art. 24.

[105] International Committee of the Red Cross (ICRC), "Convention (X) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention, The Hague, 18 October 1907," *Treaties, States Parties and Commentaries*, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=E5397A0FB560D0A9C12563CD002D6832&action=openDocument.

[106] International Committee of the Red Cross (ICRC), "Principles of International Law Recognized in the Charter of the Nüremberg Tribunal and in the Judgment of the Tribunal, 1950," *Treaties, States Parties and Commentaries*, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=854DDAACFDE285E4C12563CD002D6B95&action=openDocument.

[107] United Nations International Law Commission, Principles of International Law Recognized in the Charter of the Nüremberg Tribunal and in the Judgment of the Tribunal, July 29, 1950, Principle 6, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/854DDAACFDE285E4C12563CD002D6B95/FULLTEXT/IHL-58-EN.pdf.

[108] United Nations International Law Commission, Principles 3, 4.

Cultural Property Convention and Protocol, 1954

- *Jus in bello*: respect for cultural property within territory of all states parties, including prevention of looting or vandalism of such property;[109] visible marking (Figure 6.1) of cultural property and persons responsible for its protection;[110] protection is lost when cultural property is used for military purposes;[111] protection extends to non-international armed conflicts[112]
- Cultural property: expands and clarifies what is covered by the term *cultural property*;[113] preparations to protect such property should be done before the next onset of hostilities[114]

International Covenant on Civil and Political Rights, 1966

- Human rights:
  - rights to: life,[115] "liberty and security of the person,"[116] "respect for the inherent dignity of the human person,"[117] equality before the law,[118] presumption of innocence,[119] due process in criminal proceedings,[120] peaceful assembly,[121] marry and "found a fam-

[109] United Nations Educational, Scientific and Cultural Organization (UNESCO), Convention for the Protection of Cultural Property in the Event of Armed Conflict, The Hague, May 14, 1954, 249 UNTS 215, Art. 4, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/2A07EB0EAA5CECACC12563CD002D6BC8/FULLTEXT/IHL-60-EN.pdf (hereafter cited as Cultural Property Convention).

[110] Cultural Property Convention, Art. 6, 10, 15–17.

[111] Cultural Property Convention, Art. 8(3), 9, 11.

[112] Cultural Property Convention, Art. 19(1).

[113] Cultural Property Convention, Art. 1.

[114] Cultural Property Convention, Art. 3, 7.

[115] United Nations General Assembly, International Covenant on Civil and Political Rights, December 16, 1966, 999 UNTS 171, Art. 6, accessed February 12, 2019, https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (hereafter cited as ICCPR).

[116] ICCPR, Art. 9(1).

[117] ICCPR, Art. 10(1).

[118] ICCPR, Art. 14(1), 26.

[119] ICCPR, Art. 14(2).

[120] ICCPR, Art. 14(3).

[121] ICCPR, Art. 21.

ily,"[122] participation in public affairs and elections,[123] access public services,[124] participation in their cultural, religious, or linguistic communities,[125] state protection of rights and means of redressing violations[126]

- freedom of: movement and residence[127] (including leaving any country[128]), "thought, conscience and religion,"[129] opinion and expression,[130] association with others (including trade unions),[131]
- freedom from: torture,[132] slavery,[133] "arbitrary arrest or detention,"[134] "arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation,"[135] "propaganda for war,"[136] "advocacy of . . . hatred that constitutes incitement to discrimination, hostility or violence,"[137] forced marriage,[138] arbitrary discrimination[139]
- children's right to: having their birth recorded,[140] a name,[141] a nationality,[142] "protection as . . . required by his status as a minor"[143]
- collective rights to self-determination with respect to political status and use of natural resources[144]

[122] ICCPR, Art. 23(2).
[123] ICCPR, Art. 25(*a*),(*b*).
[124] ICCPR, Art. 25(*c*).
[125] ICCPR, Art. 27.
[126] ICCPR, Art. 2(2),(3).
[127] ICCPR, Art. 12(1).
[128] ICCPR, Art. 12(2).
[129] ICCPR, Art. 18.
[130] ICCPR, Art. 19.
[131] ICCPR, Art. 22.
[132] ICCPR, Art. 7.
[133] ICCPR, Art. 8.
[134] ICCPR, Art. 9(1).
[135] ICCPR, Art. 17(1).
[136] ICCPR, Art. 20(1).
[137] ICCPR, Art. 20(2).
[138] ICCPR, Art. 23(3).
[139] ICCPR, Art. 2(1), 26.
[140] ICCPR, Art. 24(2).
[141] ICCPR, Art. 24(2).
[142] ICCPR, Art. 24(3).
[143] ICCPR, Art. 24(1).
[144] ICCPR, Art. 1.

- Provides for limited derogation (non-recognition) of certain (but not all) rights "[i]n time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed" and made known to other states parties[145]
- Builds on foundation established by Universal Declaration[146]
- Still in force

International Covenant on Economic, Social, and Cultural Rights, 1966

- Human rights:
  - Right to: work at a freely-chosen occupation[147] under "just and favourable conditions,"[148] form and join trade unions,[149] "social security, including social insurance,"[150] an "adequate standard of living,"[151] "enjoyment of the highest attainable standard of physical and mental health"[152] (including access to health care[153]), free primary education (with states progressing toward free secondary and higher education),[154] participation in cultural life (including "benefits of scientific progress" and protection for creators' interests in their works)[155]
  - Freedom from: arbitrary discrimination,[156] hunger,[157] forced marriage[158]

---

[145] ICCPR, Art. 4.

[146] ICCPR, preamble.

[147] United Nations General Assembly, International Covenant on Economic, Social and Cultural Rights, December 16, 1966, 993 UNTS 3, Art. 6, accessed June 26, 2018, `https://treaties.un.org/doc/Treaties/1976/01/19760103%2009-57%20PM/Ch_IV_03.pdf` (hereafter cited as ICESCR).

[148] ICESCR, Art. 7.

[149] ICESCR, Art. 8(1)(*a*).

[150] ICESCR, Art. 9.

[151] ICESCR, Art. 11(1).

[152] ICESCR, Art. 12(1).

[153] ICESCR, Art. 12(2)(*d*).

[154] ICESCR, Art. 13(1),(2).

[155] ICESCR, Art. 15(1).

[156] ICESCR, Art. 2(2), 3.

[157] ICESCR, Art. 11(2).

[158] ICESCR, Art. 10(1).

    - Collective rights: of peoples to self-determination with respect to political status and use of natural resources,[159] of trade unions to operate freely (including joining other associations and calling workers to strike)[160]
- Recommendations that states provide: paid maternity benefits,[161] protection of children "from economic and social exploitation"[162]
- Builds on foundation established by UN Charter and Universal Declaration[163]
- Still in force

Outer Space Treaty, 1967

- *Jus in bello*: prohibitions on placing weapons of mass destruction in orbit around the earth or on any celestial body and on establishing military infrastructure on celestial bodies[164]

Protocols Additional to the Geneva Conventions, 1977

- *Jus ad bellum* and *jus in bello*: *attack* defined as an "act[] of violence against the adversary, whether in offence or defence"[165]
- *Jus in bello*:
    - reaffirms Martens Clause'[166'=latex

[159] ICESCR, Art. 1.

[160] ICESCR, Art 8(1)(*b*)–(*d*).

[161] ICESCR, Art. 10(2).

[162] ICESCR, Art. 10(3).

[163] ICESCR, preamble.

[164] United Nations, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, January 27, 1967, 610 UNTS 205, Art. 4, accessed November 28, 2019, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html (hereafter cited as Outer Space Treaty).

[165] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), Geneva, June 8, 1977, 1125 UNTS 3, Art. 49(1), accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/D9E6B6264D7723C3C12563CD002D6CE4/FULLTEXT/AP-I-EN.pdf (hereafter cited as AP I).

[166] AP I, Art. 1(2).

- responsibility under laws of armed combat: armed forces' codes of discipline "shall enforce compliance with the rules of international law applicable in armed conflict";[167] parties obliged to have legal advisors available to military commanders for interpretation and application of relevant laws;[168] parties obliged to determine if uses of "a new weapon, means or method of warfare . . . would . . . be prohibited";[169] parties obliged to take precautions to ensure targets are lawful and minimize "incidental loss of civilian life, injury to civilians and damage to civilian objects";[170] violations of laws of armed conflict do not terminate rights associated with being a combatant or prisoner of war[171]
- principle of distinction: protections for persons in the context of non-international armed conflicts;[172] clarification of the principle ("The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations."[173]) extension of scope of GC I–IV (1949) to "armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination";[174] extension of protections to civilian medical personnel, units, and transports, and to civilian religious personnel[175] (including those affected by non-international armed conflicts[176]); exclusion of mercenaries as com-

[167] AP I, Art. 43(1).

[168] AP I, Art. 82.

[169] AP I, Art. 36.

[170] AP I, Art. 57.

[171] AP I, Art. 44(2).

[172] International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), Geneva, June 8, 1977, 1125 UNTS 609, Art. 1(1), accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/AA0C5BCBAB5C4A85C12563CD002D6D09/FULLTEXT/AP-II-EN.pdf (hereafter cited as AP II).

[173] AP I, Art. 51(1); AP II, Art. 13(1).

[174] AP I, Art. 1(4).

[175] AP I, Art. 8, 12, 15.

[176] AP II, Art. 9, 11.

batants;[177] civilian protections for journalists;[178] restriction of military operations to those directed "only against military objectives";[179] prohibitions on attacking or terrorizing civilian persons,[180] attacking civilian objects,[181] indiscriminate attacks,[182] and reprisals against civilian persons and objects[183]

- unnecessary harm or suffering: prohibition of "methods and means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment";[184] prohibition of starvation and deprivation of "objects indispensable to the survival of the civilian population" as a means of war;[185] protection of "[w]orks or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations"[186]

- *Jus post bellum*: "grave breaches" of the conventions and protocols are to be prosecuted as war crimes[187]
- Humanitarian rules: provision for and protection of civil defence[188] and civilian relief operations;[189] protection of stateless persons and refugees;[190] measures to reunite families;[191] protections and provisions for "persons deprived of their liberty for reasons related to the [non-international] armed conflict";[192] provision of humane treatment and medical care for "[a]ll the sick, wounded, and shipwrecked, whether or not they have taken part in the [non-international] armed conflict"[193]

[177] AP I, Art. 47.
[178] AP I, Art. 79.
[179] AP I, Art. 48.
[180] AP I, Art. 51(2); AP II, Art. 13(2).
[181] AP I, Art. 52(1).
[182] AP I, Art. 51(4).
[183] AP I, Art. 51(6); AP I, Art. 52(1).
[184] AP I, Art. 35(3); *cf.* Art. 55.
[185] AP I, Art. 54; AP II, Art. 14.
[186] AP I, Art. 56(1); AP II, Art. 15.
[187] AP I, Art. 85.
[188] AP I, Art. 61–67.
[189] AP I, Art. 68–71.
[190] AP I, Art. 73.
[191] AP I, Art. 74.
[192] AP II, Art. 5.
[193] AP II, Art. 7.

- Human rights: protection for basic rights and respect for human dignity;[194] due legal process and presumption of innocence for those charged with "criminal offences related to the [non-international] armed conflict[195]
- Cultural objects: prohibition of "acts of hostility directed against the historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples"[196]
- Still in force

Convention Prohibiting Certain Conventional Weapons, 1980

- *Jus in bello*: reaffirmation of Martens Clause;[197] individual protocols prohibit the use of weapons that "injure by fragments which in the human body escape detection by X-rays";[198] the use of mines, booby-traps and other explosive devices in an indiscriminate fashion or that are designed to cause "superfluous injury or unnecessary suffering";[199]

[194] AP I, Art. 75; AP II, Art. 4.

[195] AP II, Art. 6.

[196] AP I, Art. 53; AP II, Art. 16.

[197] United Nations, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Geneva, October 10, 1980, 1342 UNTS 137, preamble, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/7A690F9945FF9ABFC12563CD002D6D8E/FULLTEXT/IHL-81-EN.pdf (hereafter cited as Conventional Weapons Convention).

[198] United Nations, Protocol on Non-Detectable Fragments (Protocol I) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, October 10, 1980, 1342 UNTS 168, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/CFCC9F92E14E1945C12563CD002D6DA9/FULLTEXT/IHL-82-EN.pdf (hereafter cited as Conventional Weapons Protocol I).

[199] United Nations, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices As Amended (Protocol II Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects), May 3, 1996, 2048 UNTS 93, Art. 3, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/82CF2C7C75E37C5AC12563FB006181B4/FULLTEXT/IHL-92-EN.pdf (hereafter cited as Conventioal Weapons Protocol II (amended)).

the use of incendiary weapons to target civilians, civilian objects, or military targets in close proximity to a "concentration of civilians";[200] the use of laser weapons or systems to induce permanent blindness[201]

- *Jus post bellum*: states participating in an armed conflict must record locations of explosive ordnance used in the conflict and provide for the removal of unexploded or abandoned ordnance after the end of hostilities[202]
- Still in force

[200] United Nations, Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons (Protocol III) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, October 10, 1980, 1342 UNTS 171, Art. 2, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/1E37E38A51A1941DC12563CD002D6DEA/FULLTEXT/IHL-84-EN.pdf (hereafter cited as Conventional Weapons Protocol III).

[201] United Nations, Protocol on Blinding Laser Weapons (Protocol IV) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, October 13, 1995, 2024 UNTS 163, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/70D9427BB965B7CEC12563FB0061CFB2/FULLTEXT/IHL-91-EN.pdf (hereafter cited as Conventional Weapons Protocol IV).

[202] United Nations, Protocol on Explosive Remnants of War (Protocol V) Annexed to the Convention on Prohbitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, November 28, 2003, 2399 UNTS 100, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/22EFA0C23F4AAC69C1256E280052A81F/FULLTEXT/IHL-99-EN.pdf (hereafter cited as Conventional Weapons Protocol V).

Convention Against Torture, 1984

- Human rights: establishes a definition of *torture*;[203] declares that torture, attempts to commit torture, and participation or complicity in torture are to be treated as crimes by states party to the convention;[204] grants victims of torture rights to redress and compensation;[205] obliges states to take steps to prevent not only torture but also "other acts of cruel, inhuman or degrading treatment or punishment which do not amount to torture as defined" in the convention[206]
- Still in force

Convention on the Rights of the Child, 1989

- *Jus in bello*: children younger than 15 years cannot be recruited into the armed forces or participate in hostilities[207]
- Human rights:
  - rights to: a name, a nationality, and parental care;[208] have their births registered;[209] expeditious re-establishment of identity if el-

[203] "The term 'torture' means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity." United Nations General Assembly, Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, December 10, 1984, 1465 UNTS 85, Art. 1, accessed January 5, 2021, https://www.ohchr.org/Documents/ProfessionalInterest/cat.pdf (hereafter cited as Convention Against Torture).

[204] Convention Against Torture, Art. 4.

[205] Convention Against Torture, Art. 14.

[206] Convention Against Torture, Art. 16.

[207] United Nations General Assembly, Convention on the Rights of the Child, November 20, 1989, 1577 UNTS 3, Art. 38, accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/B92BDC3CAE1B142DC12563CD002D6E8C/FULLTEXT/IHL-86-EN.pdf (hereafter cited as Rights of the Child).

[208] Rights of the Child, Art. 7.

[209] Rights of the Child, Art. 7.

ements of it are lost;[210] "benefit from child-care services and facilities for which they are eligible";[211] "special protection and assistance provided from the State" if their best interests are served by removal from the family environment[212]

- Still in force

Chemical Weapons Convention, 1993

- *Jus in bello*: prohibits use of weapons intended to disperse chemicals[213] "that can cause death, temporary incapacitation or permanent harm to humans or animals"[214]
- Prohibits production, accumulation, and transfer of such weapons,[215] and requires their destruction[216]
- Still in force

San Remo Manual (Armed Conflict at Sea), 1994

- Intended to be an updated version of *Oxford Manual* (1913)[217]
- Adapts developments in laws of armed conflict and other treaties since 1913 to the context of naval warfare
- Articulates protections from naval attacks for civilians at sea or in aircraft over the sea equivalent to those afforded civilians on land by GC II and AP I[218]

---

[210] Rights of the Child, Art. 8.

[211] Rights of the Child, Art. 18(3).

[212] Rights of the Child, Art. 20.

[213] United Nations, Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Paris, January 13, 1993, 1974 UNTS 45, Art. 1(1), 2(1), accessed January 3, 2021, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/xsp/.ibmmodres/domino/OpenAttachment/applic/ihl/ihl.nsf/9D3CCA7B40638EF5C12563F6005F63C5/FULLTEXT/IHL-87-EN.pdf (hereafter cited as Chemical Weapons Convention).

[214] Chemical Weapons Convention, Art. 2(2).

[215] Chemical Weapons Convention, Art. 1(1).

[216] Chemical Weapons Convention, Art. 1(2),(3).

[217] International Institute of Humanitarian Law, *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, ed. Louise Doswald-Beck (Cambridge, UK: Cambridge University Press, 1985), 5 (hereafter cited as *San Remo Manual*).

[218] *San Remo Manual*, 5.

- Not treaty law as presented, but an expression and explanation of it

Rome Statute of the International Criminal Court, 1998

- *Jus post bellum*: a permanent court with "jurisdiction over persons for the most serious crimes of international concern,"[219] in particular, genocide,[220] crimes against humanity,[221] war crimes,[222] and "the crime of aggression"[223]
- Only for cases where a state party with jurisdiction is not willing or able to investigate and prosecute in accordance with its international obligations,[224] or where a state party or the UN Security Council has referred it to the court[225]
- Still in force

Covenant for the Safeguarding the Intangible Cultural Heritage, 2003

- Cultural heritage: aims to ensure respect for and preservation of "the practices, representations, expression, knowledge, skills—as well as the instruments, objects, artefacts and cultural spaces associated therewith—that communities, groups, and in some cases, individuals recognize as part of their cultural heritage"[226] such as "oral traditions and expressions, . . . language . . . [,] performing arts . . . [,] social practices, . . . [and] traditional craftsmanship"[227]
- Still in force

[219] International Criminal Court (ICC), Rome Statute of the International Criminal Court, 2011, 2187 UNTS 90, amended, The Hague, NL, Art. 1, accessed April 8, 2020, https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf.

[220] International Criminal Court (ICC), Art. 6.

[221] International Criminal Court (ICC), Art. 7.

[222] International Criminal Court (ICC), Art. 8.

[223] International Criminal Court (ICC), Art. 8 *bis*, added in 2010.

[224] International Criminal Court (ICC), Art. 17.

[225] International Criminal Court (ICC), Art. 13.

[226] United Nations Educational, Scientific and Cultural Organization (UNESCO), Convention for the Safeguarding of the Intangible Cultural Heritage, Paris, October 17, 2003, Art. 2(1), accessed March 4, 2021, https://ich.unesco.org/en/convention (hereafter cited as CICH).

[227] CICH, Art. 2(2).

ICRC Study on Customary International Humanitarian Law, 2005

- Codification of non-treaty humanitarian law arising from near-universal practices of states with respect to particular issues[228]
- Sets out the state practices that led to the formation of each rule[229]
- Not new law, and not a substitute for treaty law, but authoritative because states largely abide by the rules set out

HPCR Manual (Air and Missile Warfare), 2009

- Codification of existing international law controlling air and missile warfare[230]
- *Jus in bello*: observes that "[t]here is no specific obligation on Belligerent Parties to use precision guided weapons. There may, however, be situations in which the prohibition of indiscriminate attacks, or the obligation to avoid—or in any event, minimize—collateral damage, cannot be fulfilled without using precision guided weapons";[231] applies rules to uncrewed aerial vehicles[232]
- Not treaty law as presented, but an expression and explanation of it

---

[228] International Committee of the Red Cross (ICRC), *Rules*, vol. 1 of *Customary International Humanitarian Law*, ed. Jean-Marie Henckaerts and Louise Doswald-Beck (Cambridge, UK: Cambridge University Press, 2005), xxxvi, accessed April 20, 2018, `https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf`.

[229] International Committee of the Red Cross (ICRC), *Practice*, vol. 2 of *Customary International Humanitarian Law*, ed. Jean-Marie Henckaerts and Louise Doswald-Beck (Cambridge, UK: Cambridge University Press, 2005), accessed April 20, 2018, `https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-ii-icrc-eng.pdf`.

[230] Claude Bruderlein, The Program on Humanitarian Policy and Conflict Research at Harvard University, *HPCR Manual on International Law Applicable to Air and Missile Warfare* (New York, NY: Cambridge University Press, 2013), vii (hereafter cited as *HPCR Manual*).

[231] *HPCR Manual*, Rule 8.

[232] *HPCR Manual*, Rule 22(a), 29(vi), 39, 147, 170.

Tallinn Manual (Tallinn 1.0 on Cyberwarfare), 2013

- Codification of existing international laws of armed conflict applied to cyberwarfare construed as "cyber-to-cyber operations"[233]
- Application of international law to a new domain of conflict, following the pattern established by *Oxford Manual* (1880), *Oxford Manual* (1913), *San Remo Manual*, and *HPCR Manual*
- *Jus ad bellum*: rules concerning self-defence or UN Security Council resolutions in response to cyberattacks[234]
- *Jus in bello*: adapts principles controlling conventional means and methods of war to cyberwarfare
- Not treaty law as presented, but an expression and interpretation of it
- Superseded by *Tallinn 2.0*

Tallinn Manual (Tallinn 2.0 on Cyber Operations), 2017

- Most comprehensive manual of applied international law to date
- Extends rules of cyberwarfare in *Tallinn 1.0* to include codification of international human rights law,[235] laws of international responsibility,[236] diplomatic and consular law,[237] the law of the sea,[238] air and space law,[239] and international telecommunications law[240] applicable to cyber-to-cyber operations in general
- Not treaty law, but an expression and interpretation of it that extends beyond the laws of armed conflict

---

[233] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge, UK: Cambridge University Press, 2013), 5, accessed September 18, 2015, `http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf` (hereafter cited as *Tallinn 1.0*).

[234] *Tallinn 1.0*, Rules 10–19.

[235] Michael N. Schmitt and Liis Vihul, eds., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge, UK: Cambridge University Press, 2017), Rules 34–38 (hereafter cited as *Tallinn 2.0*).

[236] *Tallinn 2.0*, Rules 14–31.

[237] *Tallinn 2.0*, Rules 39–44.

[238] *Tallinn 2.0*, Rules 45–54.

[239] *Tallinn 2.0*, Rules 55–60.

[240] *Tallinn 2.0*, Rules 61–64.

- *Jus in bello*: prohibits threatened or actual use of "nuclear weapons or other nuclear explosive devices"[241]
- *Jus post bellum*: provision of medical, psychological, and social assistance to victims of nuclear weapons or nuclear explosive devices;[242] obligation to decontaminate and remediate "areas . . . contaminated as a result of activities related to the testing or use of nuclear weapons or other nuclear explosive devices";[243] declaration that states parties with the resources and ability to assist other states parties in these areas shall do so[244]
- Prohibitions on: development, production, accumulation, testing, possession, and transfer of nuclear weapons or explosive devices;[245] other parties' use of state party's territory for "stationing, installation, or deployment" of these weapons or devices[246]
- Obligation for states parties to remove and destroy nuclear weapons and nuclear explosive devices[247]
- Entered into force in January 2021

[241] United Nations, Treaty on the Prohibition of Nuclear Weapons, July 7, 2017, Art. 1(d), accessed December 19, 2020, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/209/73/PDF/N1720973.pdf (hereafter cited as Nuclear Weapons Treaty).

[242] Nuclear Weapons Treaty, Art. 6(1).

[243] Nuclear Weapons Treaty, Art. 6(2).

[244] Nuclear Weapons Treaty, Art. 7(1)–(4).

[245] Nuclear Weapons Treaty, Art. 1(a)–(c).

[246] Nuclear Weapons Treaty, Art. 1(g).

[247] Nuclear Weapons Treaty, Art. 4(2),(4).

Appendix B

3-Minute Thesis transcript

How many of you have had to replace a lost or stolen credit card? A driver's licence? A birth certificate? You have to spend a lot of time proving you are who you claim to be—or if your identity has been stolen, proving who you aren't. Now imagine doing this when the official record of your birth has been destroyed—erased by a cyberattack on your government's vital statistics database.

My project explores what international laws of war such as the Geneva Conventions allow and disallow in cyberwarfare. These laws clearly state that, with rare exception, it is not lawful for one state to destroy another state's civic buildings and objects of national and cultural significance. This protects works of art, libraries, and archives like this one (Figure B.1). And this matters because when the war ends, the non-combatants can not only pick up the pieces of their lives, but also rebuild their society.

Digital archives have the same protection, even though they are not mentioned in these decades-old laws. But there is no practical way to distinguish a data centre that serves only civilian purposes from one that could be used by the military. Current military thinking says that makes them lawful targets in war. These data centres can be destroyed by a bomb strike, or by a network-based attack on the computers and storage devices. A state can destroy the vital and other historical records of another state's citizens and justify it as acceptable damage from a lawful cyberattack against a military facility.

These records are vital for rebuilding a civil society. They tell us who has the rights of citizenship, access to services, the ability to have paid work, the

Figure B.1: Vedran Smailović, "The Cellist of Sarajevo." Smailović is playing in the ruins of the National and University Library of Bosnia and Herzegovina in Sarajevo. The library had been destroyed by Serbian forces on August 25, 1992. (Photograph by Mikhail Evstafiev, available at `https://en.wikipedia.org/wiki/Vedran_Smailović#/media/File:Evstafiev-bosnia-cello.jpg` under CC BY-SA 3.0, used here by permission.)

---

freedom to travel. My research will show that international law must protect these kinds of digital objects from cyberattacks. Why does this matter? For two reasons: one for the person, and one for society. A civil society cannot exist without people being able to live well together. And you cannot live well without a home, an income, and a verifiable identity of your own. Defending your well-being requires preserving and protecting your basic personal data—the record of your identity. You are worth making sure international law is strong enough to keep warring states from destroying it.