CYBER-NUISANCE

FREDERIC GILLES SOURGENS*

ABSTRACT

2020, the year of the unprecedented SolarWinds hack, saw state-sponsored cyber-agents taking near-war tensions between the U.S. and Iran to a computer near you; inevitably, cyber-criminals are likely to exploit the ensuing chaos to hack, steal, and ransom with impunity. As it stands, the dominant cyberlaw paradigm as expressed in the 2017 NATO-led Tallinn Manual 2.0 has no realistic means to respond to or prevent these scenarios: it is stuck choosing between escalating cyber-reprisals on the one hand (sometimes conveniently or falsely attributing criminal cyber-conduct to state agents to justify a response) and paralysis to avoid such escalation on the other.

This Article submits that the cyberlaw paradigm is stuck in a false dichotomy—and that this false dichotomy can only be resolved if we gain a better understanding of the legal nature of cyberspace itself. The Article is the first to establish that cyberspace as a matter of property law consists of a global web of correlative rights protected by means of a general nuisance principle. The Article uses a functional comparative property and natural-resource law analysis to prove the existence of such a general nuisance principle premised upon the idea of correlative rights. It demonstrates that this principle is applicable to cyberspace and is in fact consistent

* Senator Robert J. Dole Distinguished Professor of Law & Director, Oil and Gas Law Center, Washburn University School of Law. I would like to thank Teddy Baldwin, David Baron, Diane Desierto, Kabir Duggal, Burke Griggs, Craig Martin, and Joseph A. Schremmer for agreeing to review early drafts of the article. I would also like to thank the *University of Pennsylvania Journal of International Law* editors for their amazing work and support.

with many of the existing starting points of cyberlaw. But it maps further how and where the Tallinn 2.0 paradigm went demonstrably astray—and more importantly, how the cyberlaw-paradigm can now be set right. Centrally, Cyber-Nuisance develops (1) how states and apex non-state actors (Windows, Apple, Facebook, Twitter, Google, and the like) share in governance obligations; (2) what the overarching goal of these governance obligations is—the protection of connectivity of cyberspace participants; and (3) an abatement-based enforcement mechanism that escapes the escalation trap bedeviling the Tallinn 2.0 approach.

The Article meaningfully advances the literature by providing a more precise legal framework for understanding the nature of cyberspace and the obligation of state and non-state actors alike to protect it. This framework can explain an intuitive insight about cyberspace that so far has escaped cyberlaw paradigms—namely, that cyberspace is at once a local and a global domain giving rise to local and global rights and obligations. The Article does so in a noticeable departure from dominant cyberlaw frameworks by grounding the analysis of cyberspace in comparative property law. It uses this lens to explain how the apparently contradictory local and global aspects of cyber are but flipsides of how one approaches correlative rights in their new, virtual context.

TABLE OF CONTENTS

I. INTRODUCTION

Many great cultures have a common utopian myth: somehow technology can overcome our limitations, somehow human ingenuity can unite mankind, somehow technology can make us masters of our universe. The Middle East had Babel and its tower.[1] Plato and the Greeks had Atlantis.[2] China arguably combines elements of both.[3]

When they write the story of our civilization, it is not difficult to guess what will take the place of our tower of Babel, our Atlantis, our attempt to unite mankind and, to put it in terms of the old myths, rival the act of creation through human ingenuity: cyberspace. Cyberspace is the dream of a united humanity outgrowing crude national competition.[4] Cyberspace is the creation of a new virtual reality to supplant the shortcomings of the physical—to allow us to connect across global divides and harness technological power to command our environment.[5]

But any student of ancient history—or casual fan of adventure movies—knows how the story ends. The tower crumbles.[6] The city sinks.[7] Civilizations fall into deep division.[8] The ambition to build a utopia is swallowed up in a wave of water or dust. A combination of arrogance or *hubris*, divine fury or natural disaster, cast them down.[9]

---

1 Genesis 11:1-9; Brent A. Strawn, *Holes in the Tower of Babel*, OXFORD BIBLICAL STUD. ONLINE, https://global.oup.com/obso/focus/focus_on_towerbabel/ [https://perma.cc/AJ2S-CX4N] (last visited Jan. 1, 2020).

2 Plato, *Critias*, *in* PLATO, THE COMPLETE WORKS 1292, 1306 (John M. Cooper ed., 1997); Mark Cartwright, *Atlantis*, ANCIENT HIS. ENCYCL. (Apr. 8, 2016), https://www.ancient.eu/atlantis/ [https://perma.cc/4RQZ-WLW7] (providing a fuller introduction to the reception of the Atlantis myth).

3 *See* Ricardo Lewis, *Does Chinese Civilization Come From Ancient Egypt?*, FOR. POL'Y (Sept. 2, 2016), https://foreignpolicy.com/2016/09/02/did-chinese-civilization-come-from-ancient-egypt-archeological-debate-at-heart-of-china-national-identity/ [https://perma.cc/U4WC-5R27] (discussing interpretations of the *Records of the Grand Historian* linking China to an Egyptian origin story).

4 *See* John Perry Barlow, *A Declaration of Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/ZHT2-GLMG].

5 *See id.*

6 Genesis 11:9, *supra* note 1.

7 Cartwright, *supra* note 2.

8 Strawn, *supra* note 1.

9 Strawn, *supra* note 1; PLATO, *supra* note 2, at 1306.

When one looks at the state of cyberattacks today it is not hard to think that our sky, too, is falling. The tools we hoped would bring us together around visions of a shared humanity have amplified our means and appetite to dehumanize even our closest neighbors.[10] And the tools we hoped would make our lives better and easier have instead become the means to rob us,[11] imperil our critical infrastructure,[12] surveil and potentially blackmail us,[13] and even turn household items into weapons against us.[14]

Not only that, but the tools we had hoped would take us beyond the nation state have become some of its most potent weapons.

---

[10] Jon Keegan, *Blue Feed, Red Feed: See Liberal Facebook and Conservative Facebook, Side by Side*, WALL STR. J. (Aug. 19, 2019), http://graphics.wsj.com/blue-feed-red-feed/ [https://perma.cc/23DC-WK7J].

[11] Hugh Son, *Jamie Dimon's worst fears for the banking industry realized with Capital One data hack*, CNBC (July 30, 2019, 2:59 PM EDT), https://www.cnbc.com/2019/07/30/jamie-dimons-worst-fears-for-banks-realized-with-capital-one-hack.html [https://perma.cc/Y6MM-U958].

[12] Nicole Perlroth & Scott Shane, *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*, N.Y. TIMES (May 25, 2019), https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html [https://perma.cc/LW57-W6C9].

[13] Neil Vigdor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, N.Y. TIMES (Nov. 11, 2020), https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html [https://perma.cc/5Q99-9LT8]; Jack Schofield, *I got a phishing email that tried to blackmail me – what should I do?*, GUARDIAN (Jan. 17, 2019, 3:00 PM EST), https://www.theguardian.com/technology/askjack/2019/jan/17/phishing-email-blackmail-sextortion-webcam [https://perma.cc/WVV3-6ZPZ].

[14] Lily Hay Newman, *Hackers Can Turn Everyday Speakers Into Acoustic Cyberweapons*, WIRED (Aug. 11, 2019, 5:07 PM), https://www.wired.com/story/acoustic-cyberweapons-defcon/ [https://perma.cc/YVR6-6T2Y].

States use cyber operations to spy,[15] sabotage,[16] and threaten.[17] They can use cyber operations to influence behavior.[18] And they use cyber operations to attack the foundations of democratic civil society.[19] Given the SolarWinds attack on U.S. governmental cyber resources, the recent hacks of Covid-19 vaccine research, as well as the recent confrontation between the U.S. and Iran, it is only likely to spur States' efforts to step up such operations rather than to abandon them.[20]

---

[15] *Targeting of Visma*, COUNCIL ON FOREIGN REL. https://www.cfr.org/cyber-operations/targeting-visma [https://perma.cc/54K4-VM9P] (last visited Mar. 7, 2021); Lindsey O'Donnell, *North Korean Spear-Phishing Attack Targets U.S. Firms*, THREATPOST.COM (Sept. 13, 2019, 9:30 AM), https://threatpost.com/north-korean-spear-phishing-attack-us/148299/ [https://perma.cc/XR66-DA2Y]; Christopher Bing, Jack Stubbs & Joseph Menn, *Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts – sources*, REUTERS (June 27, 2019, 2:21 PM), https://www.reuters.com/article/us-usa-cyber-yandex-exclusive/exclusive-western-intelligence-hacked-russias-google-yandex-to-spy-on-accounts-sources-idUSKCN1TS2SX [https://perma.cc/84JA-5EQQ].

[16] Andy Greenberg, *A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems*, WIRED (Nov. 20, 2019, 7:00 AM), https://www.wired.com/story/iran-apt33-industrial-control-systems/ [https://perma.cc/9ZQ7-6VHR].

[17] Lily Hay Newman, *Russian Hackers Haven't Stopped Probing the US Power Grid*, WIRED (Nov. 28, 2018, 2:10 PM), https://www.wired.com/story/russian-hackers-us-power-grid-attacks/ [https://perma.cc/9WBC-MXG9].

[18] *See* Paris Martineau, *The WIRED Guide to Influencers: Everything you need to know about engagement, power likes, sponcon, and trust*, WIRED (Dec. 6, 2019, 10:00 AM), https://www.wired.com/story/what-is-an-influencer/?itm_campaign=BottomRelatedStories_Sections_1 [https://perma.cc/5CPP-FVPJ] (discussing the influencer phenomenon generally).

[19] *The Most Dangerous People on the Internet This Decade*, WIRED (Dec. 31, 2019, 7:00 AM), https://www.wired.com/story/most-dangerous-people-on-internet-this-decade/ [https://perma.cc/F7XM-UFU8].

[20] David E. Sanger, Nicole Perlroth & Julian E. Barnes, *As Understanding of Russian Hacking Grows, So Does Alarm*, N.Y. TIMES (Jan. 5, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html?searchResultPosition=2 [https://perma.cc/M3SL-R5NV]; Naomi Kresge & Daniele Lepido, *Cyber Attackers Leaked Covid-19 Vaccine Data After EU Hack*, BLOOMBERG (Jan. 12, 2021, 1:20 PM EST), https://www.bloomberg.com/news/articles/2021-01-12/covid-vaccine-documents-leaked-on-web-eu-drug-regulator-says [https://perma.cc/N8B2-LXQV]; Zack Doffman, *Cyber Warfare Threat Rises As Iran And China Agree 'United Front' Against U.S.*, FORBES (July 6, 2019, 3:19 AM EDT), https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/#f399adf42ebd [https://perma.cc/6TPH-2N2K]; Matthew Vann, *2020 campaigns 'under-prepared' to combat foreign cyberattacks: Experts*, ABC NEWS (Nov. 21, 2019, 5:56 AM), https://abcnews.go.com/Politics/2020-campaigns-prepared-combat-foreign-

In this environment, it is tempting to look to paradigms of cyber *security* to keep the powers we unleashed at bay. Russian, Chinese, and Iranian proposals dream of radically decoupling the internet from a global cyberspace.[21] The dominant paradigm for cyber governance is a less radical form of such a security approach to cyberspace as a whole. It is built upon a paradigm of cyber responsibility enforced by carefully calibrated, quasi-military cyber deterrence.[22] Careful not to over-threaten, it sets a high cyber-responsibility threshold to eliminate or at the very least limit cyber reprisals.[23] Much like the Russian, Chinese, and Iranian proposals, it scraps the utopias of a new technological common cyberspace belonging to all humankind.[24] Instead, it is premised upon an imposition of order and State-power to seek to control the cyber domain.[25]

It should not come as a surprise that, from a governance perspective at least, such efforts will always be second best. The carefully constructed deterrence posture is designed to keep the cyber peace between States. It also waters down any meaningful obligation to actually govern, make safe, and improve cyberspace for its users.

If one were to impose such a responsibility on States, it would be easy for hackers (whether State-sponsored or not) to target their attacks so as to make it appear that a State's violation of its cyber-responsibility permitted a cyberattack on another State's infrastructure. The dominant paradigm seeks to avoid precisely this scenario.[26] As leading experts warn, increased calls for greater responsibility are likely to lead to greater disruption, not greater

---

cyberattacks-experts/story?id=67138383 [https://perma.cc/7QAH-8HGW]; Zolan Kanno-Youngs & Nicole Perlroth, *Iran's Military Response May Be 'Concluded,' but Cyberwarfare Threat Grows*, N.Y. TIMES (Jan. 14, 2020), https://www.nytimes.com/2020/01/08/us/politics/iran-attack-cyber.html [https://perma.cc/39UH-64ZR].

[21] Justin Sherman, *Russia and Iran Plan to Fundamentally Isolate the Internet*, WIRED (June 6, 2019, 8:00 AM), https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet/ [https://perma.cc/WMY6-WNQX].

[22] INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 84 r. 14 (Michael N. Schmitt ed., 2017) ("TALLINN 2.0") (citations to Tallinn 2.0 are to page, rule (r.) and comment paragraph (¶)).

[23] *Id.*

[24] *Id.* at 11 r. 1 ¶ 5.

[25] *Id.*

[26] Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Diligence: Gentle Civilizer or Crude Destabilizer?*, 95 TEX. L. REV. 1555 (2017).

tranquility.[27] But this means that the current paradigm retreats from much of cyberspace as essentially ungovernable—suggesting that Russia, Iran, and China may be on to something when they desire simply to be able to shut it off.[28]

This leaves the question—is there a better way or are we doomed to watch our infrastructure crumble, our virtual community sink? Utopian hopes for good cyber-governance exclusively beyond the State today appear naïve.[29] But dystopian security paradigms rooted in exclusive State power do not fare any better at conserving cyberspace.[30] Their logic, too, potentially threatens cyberspace's very existence and certainly does away with its original promise.[31]

This Article suggests that there is hope yet for cyber-governance. This hope begins with a clearer understanding of what cyberspace is. Drawing on political economy literature, the Article argues that cyberspace is a commons.[32] Particularly, it suggests that cyberspace can meaningfully be analogized to water rights in the commons literature. The commons literature explains that what matters is the sustainable use of water—and the efforts that must be made by all users to maintain physical infrastructure and limit waste to secure such sustainable access.[33] This Article will submit that the same logic holds for the sustainable use of the common resource in cyberspace: its connectivity. To secure this connectivity, all cyber-users must participate in the physical maintenance of cyber-infrastructure and diligently root out destructive use of the cyber-commons.

The problem is that as of yet, there is no bridge between the commons rationale in political economy and a legal understanding of the cyber-commons. Existing frameworks either apply the wrong property paradigm or no property paradigm at all to their

---

27 *Id.* at 1558.

28 *See* Sherman, *supra* note 21.

29 *See* Andy Greenberg, *It's Been 20 Years Since This Man Declared Cyberspace Independence*, WIRED (Feb. 8, 2016, 9:58 AM), https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/ [https://perma.cc/L3UN-2XW2].

30 *See* Sherman, *supra* note 21.

31 *See* Sherman, *supra* note 21.

32 *See* ELINOR OSTROM, GOVERNING THE COMMONS, THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (2015) [hereinafter "OSTROM"]; ELINOR OSTROM, UNDERSTANDING INSTITUTIONAL DIVERSITY (2005) [hereinafter "OSTROM DIVERSITY"]. For an application of Ostrom's theory to cyberspace governance, see Scott J. Shackelford, *The Law of Cyber Peace*, 18 CHI. J. INT'L L. 1, 29-37 (2017).

33 *See* OSTROM, supra note 32, at 76-80, n. 20.

governance model of cyber. The utopian understandings would place cyberspace beyond property into a completely shared resource.[34] This precisely misunderstands the nature of the commons outlined in the political economy literature. The security paradigm reduces cyberspace to exclusive property rights—in other words, sovereignty.[35] This understanding of property rights in the security paradigm is unsustainable as a matter of property law: not even Texas oil barons could make such an absolute claim to all mineral rights they hold in fee simple determinable.[36]

This Article is the first to develop such a full property law understanding of cyber-commons to square the circle on the basis of a functional comparative property law analysis. This analysis shows that the world's leading jurisdictions recognize a commons-based property entitlement between no ownership and full ownership: correlative rights. Global property laws protect, and thus define, correlative right by means of a nuisance logic. This nuisance logic of correlative rights actively protects the commons. It further creates reservoir communities and serves to enforce sustainable community standards.

The correlative rights approach escapes traps bedeviling the dominant security paradigm and cyber-utopias. Unlike the security paradigm, cyber-nuisance does not enforce the infringement of correlative rights through potentially spiraling countermeasures. Rather, the self-help remedy for a nuisance is abatement—the removal of the nuisance to secure the commons. Hackers seeking to encourage States to resort to excessive self-help would only encourage increased efforts at conservation. Rather than a vicious circle of countermeasure begetting countermeasure, such an approach would create a virtuous circle of conservation begetting more conservation. The law allows States to govern *up*, in the sense of repairing cyberspace and hardening its defenses. It does not allow States to govern *down* by letting even more cyberspace fall into decay for fear of assuming unwanted responsibility and risk of State reprisals.

Unlike the utopias, cyber-nuisance would anchor the responsibility for governance both in State and non-State conduct.

---

[34] *See* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 518-9 (2003).

[35] TALLINN 2.0, *supra* note 22, at 11.

[36] *See* David E. Pierce, *Carol Rose Comes to the Oil Patch: Modern Property Analysis Applied to Modern Reservoir Problems*, 19 PENN STATE ENV'T. L. REV. 241, 245-46 (2011).

States have an important role to play precisely because they have jurisdiction over key parts of cyber-infrastructure and cyber conduct.[37] But a nuisance approach understands that States are not the only actors with correlative rights or correlative duties. Rather, cyber-nuisance looks to the conduct of all cyber-participants to set responsible cyber-community standards to secure sustainable cyber-community rights. This feature of cyber-nuisance—that it draws in State and non-State actors as rights-holders and participants in governance—mirrors that of political economy literature from which this Article departed.[38] It gives flesh to the theoretical concept of "polycentric governance" underpinning the political economy literature of the commons by showing how such community standards become part and parcel of legally cognizable and legally secure correlative rights.[39]

This Article is organized in six parts. Part II outlines the dominant security paradigm premised in cyber responsibility. Part III outlines the key governance blind spots for this paradigm. Part IV introduces the concept of cyber as a commons. Part V outlines how a general principle of cyber-nuisance established on the basis of comparative property law analysis conceives a cyber-commons in terms of correlative rights and the protection of these correlative rights. Part VI then concludes with the key cyber-governance implications of the cyber-nuisance correlative rights paradigm.

II. CYBER-RESPONSIBILITY

International cyber governance is a core concern for the international community.[40] In fact, it is probably fair to say that rather than suffering from a dearth of governance ideas, cyber suffers the opposite problem: an overabundance of ideas as to how

---

[37] *See* Michael Schmitt, *In Defense of Sovereignty in Cyberspace*, JUSTSECURITY.ORG (May 8, 2018), https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/ [https://perma.cc/SS6R-3X2A].

[38] OSTROM DIVERSITY, *supra* note 32, at 281-86.

[39] OSTROM DIVERSITY, *supra* note 32, at 281-86.

[40] *See The Application of International Law in Cyberspace: State of Play*, UN OFF. DISARMENT AFF. (Oct. 25, 2018), https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/ [https://perma.cc/4ZAK-BUCJ].

cyber governance does or should function.[41] There are thus many different candidates of conduct to choose from if one were to ask a cyber-expert what code governs cyber.

Despite this abundance of different approaches, one approach to cyber governance should be treated as the first among equals.[42] That governance paradigm is the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (*Tallin 2.0*).[43] Tallinn 2.0 is the result of an international law study conducted by leading cyber security experts.[44] *Tallinn 2.0* codified 154 international law rules on the conduct of cyber operations.[45]

The goal of *Tallinn 2.0* is to translate the rules governing general international law to cyber.[46] The key matrix according to which *Tallinn 2.0* seeks to achieve this translation is through the lens of responsibility.[47] It translates the general international law of state responsibility into the cyber realm.[48]

---

41 *See e.g.*, LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 20-21 (2014).

42 *See e.g.*, Molly Sauter, *Show Me on the Map Where They Hacked You: Cyberwar and the Geospatial Internet Doctrine*, 47 CASE W. RES. J. INT'L L. 63, 70 (2015) (submitting that Tallinn Manual is the dominant paradigm in cyber); *see also* Harold H. Koh, *Keynote Address: The Emerging Law of 21st Century War*, 66 EMORY L.J. 487, 504 (2017) (singling out only the Tallinn Manual 2.0 when discussing current cyber governance instruments); Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 598-652 (2018) (outlining that States' practices in response to the Tallinn rules are uneven).

43 TALLINN 2.0, *supra* note 22.

44 TALLINN 2.0, *supra* note 22, at xxiii-xvix.

45 TALLINN 2.0, *supra* note 22, at xxiii-xvix.

46 *See* Phil Spector, *In Defense of Sovereignty, in the Wake of Tallinn 2.0*, 111 AJIL UNBOUND 219, 219 (2017-2018) (explaining that the expert authors of which he was one compiled "the Tallinn translation of international law to the cyber domain."(WC:10))

47 *See* Jensen & Watts, *supra* note 26 (explaining the link between the Tallinn 2.0 approach and classic state responsibility).

48 Spector, *supra* note 46, at 219; Jensen & Watts, *supra* note 26, at 1560. One key discussion in the literature remains whether cyber is just another new technology. Thus, "the fact that human beings have developed new technologies over time, such as trains, cars, telephones, televisions, and mobile phones, does not mean that these create new 'domains' or 'spaces' which cannot be subject to existing legal rules or principles, such as tort or criminal law." (WC:46) Dapo Akande, Antonio Coco, & Talita de Souza Dias, *Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond*, EJIL TALK! (Jan. 5, 2021), https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/ [https://perma.cc/UQ7Z-L84T]. For the reasons that will become apparent in this article, cyber poses new problems beyond those of other new technologies. Translation therefore is more difficult to achieve—even if the impulse that law remains applicable is certainly apt.

This focus on responsibility means that *Tallinn 2.0* governance must answer three related questions. First, who is responsible?[49] When we speak of "responsibility," we typically look for a "culprit"—the person who deserves the blame or sometimes, though by connotation more rarely, the praise for a certain state of affairs.[50] Second, is what was done wrong or unlawful? [51] This echoes the synonyms we typically associate with responsibility: "blame, fault, liability."[52] Third, what can we do about it in a space without effective courts?[53] This links fault with remedies of self-help known in international law as countermeasures.[54]

The *Tallinn 2.0* experts begin their quest for cyber responsibility by translating a core principle of general international law to cyber: the "State bears international responsibility for a cyber related act that is attributable to the State and that constitutes a breach of an international legal obligation."[55] To determine if a state is "responsible"—that is, a culprit—is to translate the international law governing attribution to cyber.[56]

In general international law, an action is attributable to the State in five broad general instances, namely, if the acts are: (1) acts of state organs (government ministries etc.);[57] (2) acts of organs of third states placed at the disposal of the State;[58] (3) acts of persons empowered by law to exercise governmental authority acting under color of law;[59] (4) acts under the instruction, direction, or control of

---

[49] TALLINN 2.0, *supra* note 22, at 79-110.

[50] Responsibility, definition 1.a, MERRIAM-WEBSTER (2019), https://www.merriam-webster.com/dictionary/responsibility [https://perma.cc/LSR8-3TR7] (last visited Apr. 9, 2021).

[51] TALLINN 2.0, *supra* note 22, at 177-511.

[52] Responsibility, synonyms, MERRIAM-WEBSTER (2019), https://www.merriam-webster.com/dictionary/responsibility [https://perma.cc/LSR8-3TR7] (last visited Apr. 9, 2021).

[53] TALLINN 2.0, *supra* note22, at 111-135.

[54] *See* BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 97-100 (2006).

[55] TALLINN 2.0, *supra* note 22, at 84. Akande, *supra* note 48**Error! Bookmark not defined.** (discussing agreement among different approaches on this point).

[56] TALLINN 2.0, *supra* note 22, at 84.

[57] Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10, at 40-42 (2001) [hereinafter "ILC Articles"].

[58] *Id.* at 43-45.

[59] *Id.* at 42-43.

the State;[60] or (5) acts acknowledged and adopted as their own by the State.[61]

In addition to these broad categories, general international law has special rules governing insurrections and failure of governmental authority.[62] Finally, general international law provides that it is not a defense to attribution that certain conduct was in excess of official authority or in contravention to official instructions.[63]

Tallinn 2.0 translates these principles in Rule 15 governing cyber operations by state organs;[64] Rule 16 governing cyber operations by organs of third states placed at the disposal of the State;[65] and Rule 17 governing cyber operations by non-State actors.[66]

The key provision given the problem of tracing cyber conduct to specific individuals is Rule 17. It collapses ILC Articles 8 and 11 on State Responsibility into a single rule providing that conduct under the instruction, direction, or control of the State, as well as conduct adopted by the State as its own, is attributable.[67]

Having established what kind of conduct should count as State conduct, *Tallinn 2.0* then sets out to establish rules for what kind of conduct is impermissible. That is, it tries to codify international legal prohibitions. These rules run the gamut, from rules governing special regimes of international law such as human rights,[68] diplomatic and consular relations,[69] the law of the sea,[70] to the prohibition of intervention in general international law,[71] and the law of armed conflict.[72]

This leaves the question: what may a State do if it suffers an injury and the conduct leading to the injury can be attributed to another State and is internationally wrong? Given the lack of

---

60 *Id.* at 47-49.

61 *Id.* at 52-54.

62 *Id.* at 49-52.

63 *Id.* at 45-47.

64 TALLINN 2.0, *supra* note 22, at 87.

65 TALLINN 2.0, *supra* note 22, at 93.

66 TALLINN 2.0, *supra* note 22, at 94.

67 *Compare* TALLINN 2.0, *supra* note 22, at 94 *with* ILC Articles, *supra* note 57, at 47-49, 52-54.

68 TALLINN 2.0, *supra* note 22, at 179-208.

69 TALLINN 2.0, *supra* note 22, at 209-231.

70 TALLINN 2.0, *supra* note 22, at 232-258.

71 TALLINN 2.0, *supra* note 22, at 312-327.

72 TALLINN 2.0, *supra* note 22, at 373-562.

international courts of general jurisdiction, this question frequently boils down to what kind self-help a State may deploy to bring the wrongdoer to heel.[73] In general international law, this question is governed by the law of countermeasures. Such countermeasures permit States to suspend the performance of international legal obligations owed to the wrongdoer until the wrongdoer has stopped its violation of the State's international legal rights.[74] Countermeasures must be proportionate to the injury suffered.[75] Before implementing countermeasures, a State must give the wrongdoer an opportunity to cease and desist from its wrongful conduct voluntarily.[76] But in any event, the State may not threaten the use of force or violate fundamental international law norms including fundamental human rights norms.[77]

Tallinn 2.0 translates these rules on countermeasures into the cyber-context. It entitles States to take countermeasures, "whether cyber in nature or not," for the violation of an international legal obligation.[78] Consistent with general international law, the purpose of countermeasures must be to bring about the cessation of wrongful conduct.[79] *Tallinn 2.0* stresses that countermeasures may not "amount to prohibited belligerent reprisal."[80] This links the discussion of countermeasures to the threshold when a cyber-operation is akin to the use of force.[81] This threshold prohibits operations that in "[their] scale and effects are comparable to non-cyber operations rising to the level of a use of force."[82] In other words, it does not matter whether a powerplant explodes because it is hit by a bomb or malware; this, however, leaves many devastating cyber operations in play such as "cyber psychological operations intended solely to undermine confidence in a government."[83]

---

73 *See generally* Eric Posner, *The Decline of the International Court of Justice* (John M. Olin. L. & Econ., Working Paper No. 233, 2004) (discussing why "the only international court with general subject matter jurisdiction over international legal issues" has been utilized less and less frequently over time).

74 ILC Articles, *supra* note 57, at 120, 137.

75 ILC Articles, *supra* note 57, at 134-35.

76 ILC Articles, *supra* note 57, at 135-37.

77 ILC Articles, *supra* note 57, at 131-34.

78 TALLINN 2.0, *supra* note 22, at 111.

79 TALLINN 2.0, *supra* note 22, at 116.

80 TALLINN 2.0, *supra* note 22, at 122-23.

81 TALLINN 2.0, *supra* note 22, at 123.

82 TALLINN 2.0, *supra* note 22, at 330.

83 TALLINN 2.0, *supra* note 22, at 331.

Finally, *Tallinn 2.0* also insists that countermeasures must be proportionate to the injury suffered but is explicit that it does not require reciprocity of visiting the same injury on the wrongdoer as suffered by the State enacting a countermeasure.[84]

Despite this broad scope of the rules of general international law translated to cyber, it is possible to crystalize a few general principles underlying most of them. *First*, as a general rule, States may not interfere by cyber means in the affairs of other States or individuals beyond their territorial boundaries.[85] *Second*, the principle of proportionality plays a continuing rule in the regulation of cyber conduct.[86] This principle is broadly applicable in the context of measures taken in response to threats both in the inter-State sphere and in the human rights context.[87] *Third*, there remains a strong reserved domain for States to continue to exercise near absolute authority in organizing their own political system and organization.[88]

Perhaps the most controversial and important general duty contained in *Tallinn 2.0* is the duty of diligence.[89] This duty requires that the state protect others against harm from within its borders.[90] This duty of diligence, however, does not impose a duty to monitor.[91] Rather, it requires only that the State respond to circumstances of which it has actual or constructive knowledge.[92] The duty is controversial because states, understandably, do not like obligations of diligence imposed on them, given that it severely limits their range of action—and their range of plausible deniability.[93]

---

84 TALLINN 2.0, *supra* note 22, at 127-28.

85 Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, GEO. J. INT'L L. 743, 758, 760, 763, 769, 771-72, 775-76 (2017).

86 *Id*. 754, 761.

87 *Id*.

88 *Id*. at 775.

89 Jensen & Watts, *supra* note 26, at 1566-67; Jensen, *supra* note 85, at 744-76; TALLINN 2.0, *supra* note 22, at 30-50.

90 TALLINN 2.0, *supra* note 22, at 43.

91 TALLINN 2.0, *supra* note 22, at 41-42.

92 TALLINN 2.0, *supra* note 22, at 41-42.

93 Efrony & Shany, *supra* note 42, at 645-55.

III. CRACKS IN THE CODE

a. The Connectivity Blind Spot

Tallinn 2.0 runs into conceptual problems almost from the outset. The *Tallinn-2.0* approach to global cyber law is classically State-based.[94] *Tallinn 2.0* codifies international cyber law by translating general international law rules into the new cyber context.[95] International law is the law between sovereigns.[96] So international cyber law must also be exclusively the law governing State conduct.[97]

This syllogism—international law is the law between States; international cyber law is international law; thus, international cyber law is the law between States governing cyber—holds good in academic public international law and the law of armed conflict.[98] It is therefore unsurprising that it would hold sway as a foundational matter for *Tallinn 2.0*. After all, the experts drafting *Tallinn 2.0* were experts in these fields.[99]

This syllogism of course does not suggest that all non-State conduct in cyber is legally irrelevant. Quite to the contrary. It is just not an issue for *international* cyber law. It is a matter subject to the jurisdiction of domestic courts and regulation by domestic law.[100]

---

[94] *See* TALLINN 2.0, *supra* note 22, at 17 (conceiving of cyber law around the premise of violation of sovereignty).

[95] Spector, *supra* note 46, at 219.

[96] JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 14-15 (9th ed. 2019); JAMES CRAWFORD, CHANCE, ORDER, CHANGE: THE COURSE OF INTERNATIONAL LAW, GENERAL COURSE ON PUBLIC INTERNATIONAL LAW 221 (2014)("CRAWFORD 2014") ("If international law is the law *between* States (as historically conceived), and in some sense is derived beyond the control of domestic constitutional arrangements, by contrast the *locus* of validity of municipal law is a matter which is the first and usually the last place of local constitutional ordering.").

[97] TALLINN 2.0, *supra* note 22, at 17.

[98] *See* CRAWFORD, *supra* note 96, at 14-15 (general international law governs relationship between states); GARY D. SOLIS, THE LAW OF ARMED CONFLICT, INTERNATIONAL HUMANITARIAN LAW IN WAR 189 (2d ed. 2016) (law of armed conflict governs conflicts between states of a certain kind)

[99] TALLINN 2.0, *supra* note 22, at xii-xviii.

[100] CRAWFORD, *supra* note 96, at 440-470; Nori Katagiri, *Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks*, 7 J CYBER SEC. (2021), https://academic.oup.com/cybersecurity/article/7/1/tyab009/6168044 [https://perma.cc/BV5H-9HT7].

Tallinn 2.0 follows traditional international law in treating non-State conduct as an issue subject to domestic regulation.[101] Thus, international cyber law "does not extend to the actions of non-State actors unless such actions are attributable to a State."[102] It does not apply to corporate conduct.[103] It does not even apply to the conduct of terrorist groups.[104] *Tallinn 2.0* is unequivocal on this point.[105]

Tallinn 2.0 sets out that such non-State conduct is subject to the ordinary domestic criminal jurisdiction of States themselves.[106] Thus a corporation hacking a State would be subject to the criminal process of its home state.[107] Presumably, the corporation would also be subject to the criminal jurisdiction of the State at the receiving end of the hack.[108] *Tallinn 2.0*, in sum, treats non-State conduct as potentially criminal activity under domestic law and subjects international cyber-criminal prosecutions to much of the same strictures as ordinary criminal process.

This approach has a significant conceptual blind spot. *Tallinn 2.0* might work if it seamlessly imposed an obligation on the State to criminalize, monitor, and enforce cyber-crime law in its jurisdiction and cooperate with other States in the enforcement of their cyber laws. If that were the case, there would be no need for international cyber law to reach the conduct of non-State actors in order to safeguard international cyber governance: the obligation in international cyber law for domestic law to bear the brunt of cyber governance and regulation of non-State actors plausibly would fill the governance gap of a purely State-based paradigm.[109]

Problematically, *Tallinn 2.0* does not follow such an approach. To the contrary, it is explicit that the diligence principle does not imply an obligation to take preventive measures to interdict cyber harm from non-State actors.[110] What is more, there is not even an

---

101 *See* Schmitt, *supra* note 37. For additional context, see also Akande, *supra* note 48.

102 TALLINN 2.0, *supra* note 22, at 17.

103 TALLINN 2.0, *supra* note 22, at 17-18.

104 TALLINN 2.0, *supra* note 22, at 18.

105 TALLINN 2.0, *supra* note 22, at 18.

106 TALLINN 2.0, *supra* note 22, at 51.

107 TALLINN 2.0, *supra* note 22, at 17-18

108 TALLINN 2.0, *supra* note 22, at 60-66.

109 For a discussion of such a paradigm, see Frédéric G. Sourgens, *The Paris Paradigm*, 2019 U. ILL. L. REV. 1637 (2019).

110 TALLINN 2.0, *supra* note 22, at 44.

obligation to monitor cyber activity by non-State actors.[111] In short, *Tallinn 2.0* imposes no obligation on States to regulate, monitor, and enforce cyber conduct on the domestic level.[112] Its diligence obligation only covers the obligation to cease and desist or interdict *future* conduct once existing conduct has already caused significant cross-boundary adverse consequences abroad.[113]

This threshold was set with an eye towards the availability of countermeasures.[114] A low threshold for diligence obligations increases the opportunity (or excuse) for significant countermeasures.[115] Given the significant range of available cyber countermeasures outlined above, this is clearly an undesirable result.

But from any governance perspective, such a diligence obligation is too toothless to bite: it permits States to wait for significant adverse consequences before acting.[116] As far as governance design goes, this has "diligence" backwards. Diligence is an exercise in understanding risk for significant adverse consequences *before* they arise and not after.[117] The point of diligence is to "avoid nasty surprises."[118] The point of governance is to enlist stakeholders to avoid disaster to the greatest extent possible and sustainable.[119] Diligence is a tool to achieve this end. *Tallinn 2.0* diligence, unlike governance, only springs into action once there is a crisis. This fundamentally misunderstands the point of diligence.[120]

Tallinn 2.0's understanding of diligence is even more problematic in the cyber context. This problem can best be illustrated by way of example. On June 27, 2017, the world suffered

---

111 TALLINN 2.0, *supra* note 22, at 45.

112 TALLINN 2.0, *supra* note 22, at 45.

113 TALLINN 2.0, *supra* note 22, at 43.

114 Jensen & Watts, *supra* note 26, at 1563-64.

115 *See* Jensen & Watts, *supra* note 26, at 1563-64.

116 TALLINN 2.0, *supra* note 22, at 40.

117 *See* LINDA S. SPEDDING, DUE DILIGENCE AND CORPORATE GOVERNANCE 2 (2004).

118 Rodrigo Amaral, *Due diligence: making sure there are no nasty surprises*, RACONTEUR (Dec. 8, 2015), https://www.raconteur.net/finance/due-diligence-making-sure-there-are-no-nasty-surprises [https://perma.cc/WFQ7-259F].

119 MARK BEVIR, GOVERNANCE: A VERY SHORT INTRODUCTION 1-10 (2012).

120 While diligence also has a role to play in crisis management, this is not its principal role. Udaibir S. Das & Marc Quintyn, *Crisis Prevention and Crisis Management: The Role of Regulatory Governance* 42-48 (Int'l Monetary Fund, Working Paper No. 02/163, 2002).

a devastating cyberattack dubbed "NotPetya."[121] Western intelligence services believe that Russia deployed NotPetya as a cyberattack against Ukraine.[122] The Russian government steadfastly denies this charge.[123]

What is undisputed is that NotPetya spread from Ukraine to Denmark, the U.S., and India, and resulted in significant damage in the billions of dollars in all three jurisdictions.[124] All NotPetya ever needed to spread beyond Ukraine was the smallest of footholds in a *single* unprotected computer in a company to shut down and destroy that company's entire g*lobal* IT infrastructure and infect other companies continents away.[125] That is what apparently happened to Danish shipping giant Maersk, shutting down its headquarters in Copenhagen and much of the shipping on the U.S. Eastern seaboard.[126] Given the scope of the initial attack, this disruption outside of Ukraine was likely unintended.[127]

Reacting to events like NotPetya *after* they strike may well be an exercise in futility. Once the world notices serious adverse consequences from a NotPetya event, it is already too late to stop it or even mitigate the damage.[128] Therefore, to be meaningful, diligence must *prevent* cyber threats and not merely react to them.

Tallinn 2.0's State-based approach also suffers from an intuitive problem, even if it heightened state diligence obligations. Companies such as Windows, Apple, Facebook, Twitter, or Google have far greater *de facto* influence over cyber governance than a State

---

121 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [https://perma.cc/5ECZ-XMTW].

122 Ellen Nakashima, *Russian military was behind NotPetya cyberattack in Ukraine, CIA concludes*, WASH. POST (Jan. 12, 2018, 6:46 PM), 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 [https://perma.cc/DZE3-6ZWB].

123 Rachel England, *Russia denies UK claim it was behind NotPetya cyberattack*, ENGADGET (Feb. 15, 2018), https://www.engadget.com/2018/02/15/russia-denies-uk-claim-it-was-behind-notpetya-cyberattack/ [https://perma.cc/BV88-NRU8]

124 James E. Scheuermann, *Cyber Risks, Systemic Risks, and Cyber Insurance*, 122 PENN STATE L. REV. 613, 635 (2018).

125 Greenberg, *supra* note 121.

126 Greenberg, *supra* note 121.

127 Greenberg, *supra* note 121.

128 Greenberg, *supra* note 121.

such as Nepal.[129] Yet, Nepal is captured by the *Tallinn 2.0* approach but Windows, Apple, Facebook, Twitter, and Google are not.[130] This leaves a significant governance gap in the cyber fabric.[131]

NotPetya again is a good example for this problem—this time of the role of non-State actors in cyber governance. NotPetya exploited a vulnerability in a Windows protocol allowing hackers to run code remotely on a computer without a patch for the vulnerability.[132] Windows was aware of the vulnerability partly due to news reports advertising an NSA hacking tool exploiting the same vulnerability.[133] As NotPetya began its destructive work, Windows was working on releasing a patch, but the patch had not yet been fully implemented worldwide.[134] Windows thus is a key player in any governance discussion in how to avoid another NotPetya, as is the diligence of critical infrastructure companies in updating operating systems once they have been notified of a vulnerability. In other words, to focus only on Russia or only on Ukraine misses the bigger picture of the role of non-State conduct in cyber safety.

What is more, to understand NotPetya is to understand that State and non-State conduct connects and interacts on a constant basis. The NSA was the first to exploit a Windows vulnerability with its hacking tool EternalBlue.[135] Without the U.S. government-sponsored hacking tool, would NotPetya have happened? Then there is the question of the hack of the NSA by a hacking collective known as Shadow Brokers, which began leaking tools including EternalBlue from August 2016 onwards.[136] Mysterious as it is,

---

[129] *See* Daniel Dobrygowski, *Why Companies Are Forming Cybersecurity Alliances*, HARV. BUS. REV. (Sept. 11, 2019), https://hbr.org/2019/09/why-companies-are-forming-cybersecurity-alliances [https://perma.cc/2XSZ-DUGZ] (discussing cyber presence of non-state actors); Narayan Koirala, *Cybersecurity: A strategic imperative for Nepal*, KATHMANDU POST (Oct. 18, 2019, 7:58 AM), https://kathmandupost.com/columns/2019/10/18/cybersecurity-a-strategic-imperative-for-nepal [https://perma.cc/6NPS-76BD] (discussing recent cyber threats to Nepal and Nepalese cyber capabilities).

[130] TALLINN 2.0, *supra* note 22, at 40.

[131] TALLINN 2.0, *supra* note 22, at 40.

[132] Greenberg, *supra* note 121.

[133] Greenberg, *supra* note 121.

[134] Greenberg, *supra* note 121.

[135] Greenberg, *supra* note 121.

[136] Scott Shane, Nicole Perlroth & David E. Sanger, *Security Breach and Spilled Secrets Have Shaken the NSA to Its Core*, N.Y. TIMES (Nov. 12, 2017), https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html [https://perma.cc/37E9-E2TG].

Shadow Brokers apparently is a non-State actor.[137] Without this hack, would NotPetya have happened? Moreover, there is the apparently slower implementation of the Windows patch in Ukraine by multinationals.[138] Without this slow implementation would NotPetya have happened? Finally, there is the deployment of NotPetya, the origin of which remains contested. The story of NotPetya thus involves Windows, the world's leading operating system, a hacker collective, the NSA, Ukraine, multinational companies in Ukraine, and, according to Western intelligence, Russia. At each stage of development, NotPetya was possible because of an interaction between States and non-State actors. To prevent events like NotPetya, or worse than NotPetya, means to capture this interaction and connectivity between all of the players involved, not just some of them.

The same kind of problem arises in the context of what has been dubbed "the biggest espionage hack on record": SolarWinds.[139] The hack accessed critical records of at least ten government agencies, as well as multiple apex companies, such as Microsoft.[140] This operation had a clear espionage component.[141] But it is also possible that it could add "something more sinister" such as "inserting 'backdoor' access into government agencies, major corporations, the electric grid and laboratories developing and transporting new generations of nuclear weapons."[142] As one former national security official put it, hackers "will surely have used its access to further exploit and gain administrative control over the networks it considered priority targets."[143] He goes on that for "those targets,

---

137 Bruce Schneider, *Who Are the Shadow Brokers*?, ATLANTIC (May 23, 2017), https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/ [https://perma.cc/K3CJ-Y83M].

138 *See* Greenberg, *supra* note 121.

139 Brian Barret, *Security News This Week: Russia's SolarWinds Hack Is a Historic Mess*, WIRED (Dec. 19, 2020, 9:00 AM), https://www.wired.com/story/russia-solarwinds-hack-roundup/ ("Historic Mess") [https://perma.cc/G39M-C5VT].

140 Nicole Perlroth, David E. Sanger & Julian E. Barnes, *Widely Used Software Company May Be Entry Point for Huge U.S. Hacking*, N.Y. TIMES (Jan. 11, 2021), https://www.nytimes.com/2021/01/06/us/politics/russia-cyber-hack.html?searchResultPosition=2 [https://perma.cc/SZ9H-JYUE].

141 Sanger, *supra* note 20.

142 Sanger, *supra* note 20.

143 Thomas P. Bossert, *I Was the Homeland Security Adviser to Trump. We're Being Hacked*, N.Y. TIMES (Dec. 16, 2020), https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html [https://perma.cc/S38L-934E].

the hackers will have long ago moved past their entry point, covered their tracks and gained what experts call "persistent access," meaning the ability to infiltrate and control networks in a way that is hard to detect or remove."[144]

Like NotPetya, U.S. intelligence is reasonably certain that the hack was Russian government sponsored.[145] However, official statements "offered no details" and in fact "made no mention of . . . the S.V.R., Russia's most skilled intelligence agency."[146] Unofficially, the role of the S.V.R. is assumed.[147]

But also like NotPetya, this particular hack involved a great number of private entities in multiple countries. It was a "a supply-chain attack, meaning the pathway into the target networks relies on access to a supplier."[148] This supply chain attack centrally involved SolarWinds, an Austin, Texas, based cyber monitoring and management company with unrivalled access to government and corporate clients.[149] The hack used a product named "Orion" and was SolarWinds's "flagship network management software" to infiltrate targets.[150] Centrally, "SolarWinds moved much of its engineering to satellite offices in the Czech Republic, Poland and Belarus."[151] At this point, the attack involves a key private company doing business in multiple countries. Such supply chain attacks thus again highlight the crucial importance of private actors—not just government actors. And this particular attack highlights that such attacks can take place in multiple physical locations across national boundaries and thus involve a panoply of State and non-State actors in the process.

Tallinn 2.0 becomes dangerously ineffective as a governance tool because it does not fully account for this connectivity of State and non-State conduct in cyber. One could thus fairly apply the observation to cyber that "[h]ybrid arrangements like these are

---

144 *Id.*

145 *Id.*

146 Perlroth, *supra* note 140.

147 *See* Bossert, *supra* note 143.

148 Bossert, *supra* note 143.

149 *See* Raphael Satter, Christopher Bing & Joseph Menn, *Hackers used SolarWinds' dominance against it in sprawling spy campaign*, REUTERS (Dec. 15, 2020, 9:08 PM), https://www.reuters.com/article/global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUSKBN28Q07P [https://perma.cc/U763-QYA9].

150 *Id.*

151 Sanger, *supra* note 20.

likely to become more common in the twenty-first century."[152] Cyber seems to feel this strain with particular force due to the outsized role of non-State actors in controlling cyber infrastructure and attacking it in turn. One should thus worry that "[g]iven the phenomenon of hybridization, one of the challenges of international law in the twenty-first century will be to identify the circumstances in which a participatory arrangement should be pierced and the ways in which the consequences of piercing should be dealt with."[153] Here, *Tallinn 2.0* falls short.

b. The Attribution Vulnerability

Given Tallinn 2.0's State-centered approach, one of its central features is to determine whether particular conduct was in fact State conduct. As discussed in the previous section, this question is one of "attribution" in public international law.[154] As also discussed above, *Tallinn 2.0* on its face follows classic international law in attributing conduct of State organs and conduct under the instruction, direction or control of the State as well as conduct adopted as its own by the State after the fact.[155]

But *Tallinn 2.0* encounters an evidentiary problem. Cyber is different from other State conduct in that we are dealing with virtual actions rather than real ones. To explain, to determine whether an organ of State acts in the brick-and-mortar context, one would point to official documents from a Ministry.[156] To determine whether actions by non-State actors were under the instruction, direction, or control of the government in the brick-and-mortar world one looks for physical clues linking governmental authorities to the actions of a formally independent actor.[157] The task is one that follows physical clues much in the way that Sherlock Holmes did in the

---

152 W. MICHAEL REISMAN, THE QUEST FOR WORLD ORDER AND HUMAN DIGNITY IN THE TWENTY-FIRST CENTURY: CONSTITUTIVE PROCESS AND INDIVIDUAL COMMITMENT 324 (2013).

153 *Id.* at 325.

154 *See* section III(a) *supra*.

155 *Id.*

156 *See* PRZEMYSLAW SAGANEK, UNILATERAL ACTS OF STATES IN PUBLIC INTERNATIONAL LAW 335 (2015) (discussing how unilateral declarations of can create obligations for states).

157 *See* Marko Milanović, *State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plüecken*, 22 LEIDEN J. INT'L L. 307 (2009).

Victorian age[158]—with the possible difference that some of the documents previously housed in physical archives are now stored in the cloud and that letters have been replaced by emails. Still, the issue ultimately remains establishing real world conduct by "real people" and not by machines.

Tallinn 2.0 attribution does not have this luxury. Rather, the best we can do in cyber is to tie machines to actions. One example of this is the recent Mueller investigation into interference in the 2016 election and particularly the indictment against Russian operatives resulting from the probe.[159] The indictments against Russian military officers handed down by the Special Counsel were premised upon the fact that certain communications had originated from a certain accounts linked to a website infrastructure which, in turn, could be linked to a specific person.[160] Further, the indictment linked bitcoin-denominated purchases in the same way to link them back to the same individuals.[161]

No matter one's conclusions whether such indictments may lead to convictions, this type of search is reasonably different from traditional sleuthing. It tries to follow virtual breadcrumbs such as email addresses, bitcoin ledger entries, and cyber infrastructure, not brick-and-mortar breadcrumbs.[162] The Mueller investigation followed evidence of online transactions through the bitcoin ledger to establish that the bitcoin to purchase certain server space that in turn had been linked to misinformation campaigns on social media had commenced at the ominous GRU office building.[163]

The additional problem faced by this sort of investigation compared to a brick-and-mortar investigation is that it must ultimately make an inference from cyber reality to flesh-and-blood people. The problem is that hacks are intended precisely to call such inferences into question and to pretend that hackers are actually other people, working from virtual locations and cyber infrastructure other their own. In fact, that allegation was part of

---

158 *See* ARTHUR CONAN DOYLE, THE ADVENTURES OF SHERLOCK HOLMES, A SCANDAL IN BOHEMIA (2016).

159 United States v. Netyksho et al, No. 1:18-cr-00215, 2018 WL 3407381 (D.D.C. July 13, 2018).

160 *Id.* at ¶ 21.a.

161 *Id.* at ¶¶ 59-61.

162 *Id.* at ¶¶ 21.a, 59-61.

163 *Id.*

the indictment itself.[164] The conceptual problem is to distinguish between another, more cleverly disguised hack and the real person.

The problem in the attribution context is that attribution ultimately must link back to a real person. But creating this link between cyber conduct and a real person cannot rely upon traditional attribution rules, as traditional attribution rules did not typically encounter this problem. The closest classic international law comes to the same set of problems is the world of espionage and covert operations.[165] But even there, what unmasks the covert agent is physical evidence as opposed to inferences from virtual evidence.[166] Thus, even if *Tallinn 2.0* sounds conventional in following traditional international law of attribution, *Tallinn 2.0* of necessity innovates the law of attribution to provide a way to make the last leap from the virtual to the real.

Tallinn 2.0 wrestles openly with this problem. Thus, in the context of attribution of conduct by state organs to the state, it notes that while "the use of governmental assets, in particular military equipment like tanks and warships, has long constituted a nearly irrefutable indication of attribution due to the improbability of their use by persons other than State organs" this inference does not translate easily to cyber.[167] The problem is that "another State or a non-State actor may have acquired control over government cyber infrastructure."[168] Therefore, the use of cyber infrastructure only "can serve as an indication that the State in question may be associated with the operation."[169] The prevalence of spoofing makes this more than an academic concern.[170] *Tallinn 2.0* leaves it vague how attribution then is to function beyond the identification of the relevant cyber infrastructure, pointing to human intelligence and prudential factors.[171]

---

164 *Id.*

165 For a discussion of the international law of espionage, see Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L.J. 185 (Winter, 2020), which examines the legal framework for peacetime espionage and limitations.

166 *See Robert Hanssen*, FBI (Feb. 20, 2001), https://www.fbi.gov/history/famous-cases/robert-hanssen [https://perma.cc/Y4US-4PWW] (detailing how Robert Hanssen was unmasked as a covert Soviet/Russian operative and how his traditional intelligence helped to unmasked U.S. assets in Russia).

167 TALLINN 2.0, *supra* note 22, at 90 r. 15 ¶ 13.

168 TALLINN 2.0, *supra* note 22, at 90 r. 15 ¶ 13.

169 TALLINN 2.0, *supra* note 22, at 90 r. 15 ¶ 13.

170 TALLINN 2.0, *supra* note 22, at 91 r. 15 ¶ 15.

171 TALLINN 2.0, *supra* note 22, at 91-93 r. 15 ¶¶ 15-17.

This approach to attribution leaves a sour taste. Particularly, *Tallinn 2.0* points to the 2013 cyber operation to shut down South Korean banking and media servers and computers and asserts that the operation was "allegedly North Korean."[172] Shortly after that attack, hackers leaked Sony sensitive information, including employee social security numbers. The attack was originally attributed to North Korea. Since then, however, cyber experts have expressed doubts about attributing the conduct to North Korea.[173] Despite these doubts, North Korea remained a suspect for the hack.[174] This leaves two questions. The first is if there are doubts about the Sony hack, should there be doubts about the South Korean hack? Second, if attribution cannot firmly be established, then what is the consequence for *Tallinn 2.0*'s state-based, fault-based paradigm?

The same concern is only heightened in the context of attribution due to governmental instruction, direction, or control under ILC Article 8 and *Tallinn 2.0* Rule 17.[175] If it is difficult to establish action by a state organ, this difficulty is only increased in the context of indirect state action through the exercise of direction or control over formally non-State conduct. *Tallinn 2.0* notes as an example of effective control "a case in which one State plans and oversees an operation to use software updates to implant new vulnerabilities in software widely used by another State in its governmental computers. The former State concludes a confidential contract to embed the exploits with the company that produces" the software.[176]

This scenario outlined by *Tallinn 2.0* recalls the reported covert collaboration between Siemens and the German intelligence service, the *Bundesnachrichtendienst*. Siemens constructed Iran's nuclear reactor for supposedly civilian purposes. Siemens used this access to collaborate with the *Bundesnachrichtendienst* to allow German

---

172 TALLINN 2.0, *supra* note 22, at 91 r. 15 ¶ 14.

173 *See* Brian Todd & Ben Brumfield, *Experts doubt North Korea was behind Sony hack*, CNN (Dec. 27, 2014, 3:05 PM), https://www.cnn.com/2014/12/27/tech/north-korea-expert-doubts-about-hack/index.html [https://perma.cc/B3VC-TVAZ].

174 *Id.*

175 ILC Articles, *supra* note 57, at art. 8; TALLINN 2.0, *supra* note 22, at 94 r. 17.

176 TALLINN 2.0, *supra* note 22, at 95 r. 17 ¶ 7.

intelligence to spy on the Iranian nuclear program.[177] Siemens also extended this cooperation to granting the *Bundesnachrichtendienst* access to communications technology and thus allowing the agency to decrypt Iranian secret communications.[178] This collaboration also gave the *Bundesnachrichtendienst* alleged privilege access to encrypted messages from Russia, Egypt, and Oman.[179] *Tallinn 2.0* essentially updates such an intelligence cooperation from hardware (communication system provided by Siemens) to software.

In fact, Iran accused Siemens of complicity in the Stuxnet cyberattack on its nuclear centrifuges along just such grounds. Stuxnet was a worm used to infiltrate the SCADA operating system controlling centrifuges used to enrich fissile material used as fuel in nuclear reactors (or payload in a nuclear bomb).[180] The Stuxnet worm destroyed the centrifuges at the Iranian nuclear facility and reportedly was the first cyberweapon to lead to such physical destruction.[181] Iran alleged that the SCADA operating system had purposefully left a backdoor open for the attack much in the way suggested by the *Tallinn 2.0* attribution approach, relying on the past close collaboration between Siemens and intelligence services and the fact that many of the critical components in Iran's programs were made by Siemens.[182]

The problem is that many cyber operations comprise significantly more layers between the official State organs and the shadowy perpetrators executing the operation. In this context, *Tallinn 2.0* is arguably of little to no help to attribute conduct to the state: "a State's preponderant or decisive participation in the 'financing, organizing, training, supplying, and equipping . . . the

---

177 *See Ehemalige Manager packen aus*, MANAGER MAGAZIN (Apr. 12, 2008, 4:46 PM), https://www.manager-magazin.de/unternehmen/artikel/a-547036.html [https://perma.cc/5LKP-NFMJ].

178 *See* NORBERT SIEGMUND, DER MYKONOS PROZESS 31 (2000).

179 *See* Alex Benesch, *Stuxnet-Virus: Erneute Kooperation zwischen BND und Siemens?*, RECENTR.COM (Oct. 2, 2010), http://recentr.com/2010/10/02/stuxnet-virus-erneute-kooperation-zwischen-bnd-und-siemens/ [https://perma.cc/X5QY-2AGW].

180 *See Iran accuses Siemens over Stuxnet virus attack*, REUTERS (Apr. 17, 2011), https://www.reuters.com/article/us-iran-nuclear-stuxnet-idUSTRE73G0NB20110417 [https://perma.cc/7SG5-3EDN] [hereinafter *Iran Accuses Siemens*].

181 *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Mar. 11, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [https://perma.cc/P7Z4-PF34].

182 *Compare Iran Accuses Siemens*, *supra* note 180, *with* TALLINN 2.0, *supra* note 22, at 95 r. 17 ¶ 7.

selection of its military or paramilitary targets, and the planning of the whole of its operation' has been found insufficient to reach the 'effective control' threshold."[183] Ominously, this means that the cyber activities of this group are not attributable to the State.[184]

One again has to place this conceptual language into perspective. A cooperation between Siemens and the *Bundesnachrichtendienst* is arguably attributable to Germany because Germany structured its alleged cooperation through an officially sanctioned conduit (its intelligence service). But what about "patriotic hackers?" The term gained currency when President Putin of Russia was asked about Russian interference in the 2016 election. In response, "Russian President Vladimir Putin said . . . his country has 'never engaged in' hacking another nation's elections, but left open the possibility that hackers with 'patriotic leanings . . . may try to add their contribution to the fight against those who speak badly about Russia.'"[185]

Hitting precisely on *Tallinn 2.0* concepts, President Putin continued that "[h]ackers are free people, just like artists who wake up in the morning in a good mood and start painting."[186] These hackers may thus be supported by the Russian state—though President Putin did not concede as much—but they are not under the direction or effective control of the Russian State; they "are free people."[187] Their conduct therefore is not attributable to the Russian Federation.

This distinction between alleged German and alleged Russian conduct shows the serious problem for the attribution provisions in *Tallinn 2.0*. They fail to live up their promise precisely because of the first problem identified in the previous section: only State conduct is covered by *Tallinn 2.0* and *Tallinn 2.0* does not impose a duty on the State to police its own cyberspace.[188] This means that actors can collaborate with States time and time again without being subject to criminal sanction on the territories of these States.[189] And

---

183 TALLINN 2.0, *supra* note 22, at 95 r. 17 ¶ 9.

184 TALLINN 2.0, *supra* note 22, at 95 r. 17 ¶ 9.

185 Krishnadev Calamur, *Putin Says 'Patriotic Hackers' May Have Targeted U.S. Election, But He Denied the Russian State Was Involved*, THE ATLANTIC (June 1, 2017), https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/ [https://perma.cc/4RWS-X8L9].

186 *Id.*

187 *Id.*

188 TALLINN 2.0, *supra* note 22, at 44 r. 7 ¶ 7.

189 TALLINN 2.0, *supra* note 22, at 44 r. 7 ¶ 7.

yet the conduct of these non-State actors is not attributable to the State either as the State does not exercise sufficient control over the operation.[190] While at the time of this writing it is "too early to tell" how the attribution story will play out in the SolarWinds hack, similar questions will likely abound.[191]

Thus, it is one thing if the hack was perpetrated directly by a Russian state organ (although again, it is at this point not clear that it was so perpetrated even though there is significant suspicion to that effect).[192] It is another thing if it, too, was performed by freelance patriotic hackers. Such a freelance approach would certainly be possible with a pure intelligence hack[193] (former intelligence operatives sell information to the government after receiving materials from the government). It would leave more to chance to allow such freelancers to install backdoors and then sell the access after the fact. But even such a strategy would not be unheard of—Russian government officials have long been suspected of relying on complex nominee structures to dissociate themselves from sensitive but very high value transactions.[194]

Be that as it may, the fact that the hack remained undetected for as long as it did means that an intruder of any competence is likely to have cleaned up their tracks.[195] It is unlikely that backdoors will be easily discovered.[196] And given that the hack itself was not discovered in real-time, it is similarly unlikely that the hackers would have left behind significant breadcrumbs without raising suspicions that they meant to leave them.[197] In either case, the attribution analysis will be fraught with guesswork (and second guesswork).

In other words, *Tallinn 2.0* illustrates how to get between the wall and the wallpaper of the *Tallinn 2.0* approach (and thus escape

---

190 TALLINN 2.0, *supra* note 22, at 95 r. 17 ¶ 9.

191 Satter, *supra* note 149.

192 Satter, *supra* note 149; *see also* Bossert, *supra* note 143.

193 Calamur, *supra* note 185.

194 *See* DAVID E. HOFFMAN, THE OLIGARCHS: WEALTH AND POWER IN THE NEW RUSSIA 233 (2011) (discussing the theory of magic hands behind favorable business deals in Russia).

195 *See* Bossert, *supra* note 143.

196 Bossert, *supra* note 143

197 Bossert, *supra* note 143; Dan Goodin, *SolarWinds malware has "curious" ties to Russian-speaking hackers*, ARS TECHNICA (Jan. 11, 2021), https://arstechnica.com/information-technology/2021/01/solarwinds-malware-has-curious-ties-to-russian-speaking-hackers/ [https://perma.cc/4U8X-H3EE] (raising concern of false flags in SolarWinds hack).

lawful countermeasures). So long as the aid received from the State is not itself a violation of another international norm (and frequently the aid may well be innocuous enough, such as when the State provides hardware or generic training),[198] and so long as the State has plausible deniability of what "patriotic hackers" are doing,[199] and so long as these hackers make sure to take advantage of the connectivity issues in cyber discussed in the previous section, the underlying conduct is beyond the reach of the law.[200] It is therefore reasonable to suspect that these blind spots in *Tallinn 2.0*, when combined, provide a blueprint for governance avoidance as much as they provide a blueprint for a governance model.

c. The Fault Trap

Tallinn 2.0's governance avoidance problem is further exacerbated by its focus on responsibility. This focus on responsibility means that a State is only accountable if it acted wrongfully. Accordingly, the state must be at fault for it to be responsible for its conduct.

This fault paradigm constructs a dangerous governance trap. To paraphrase Yoda the Elder, fault leads to fear. Fear leads to blame. Blame leads to deflection. Deflection leads to willful blindness.[201]

Such willful blindness is one of the greatest threats to governance structures. It does not proactively make information available that could have been used to formulate accurate threat assessments and devise effective responses to avoid or mitigate the threat. In other words, it is trapped in the compartmentalization of responsibilities that led to significant intelligence failures in the U.S.

---

198 TALLINN 2.0, *supra* note 22, at 95 r. 17 ¶ 9.

199 *See id*. at 41 r. 6 ¶ 39 (setting out the threshold for constructive knowledge).

200 *See supra* section III(a).

201 *See* STAR WARS, EPISODE I: THE PHANTOM MENACE (Lucasfilm 1999) (Yoda the Elder noting that fear leads to anger and anger leads to suffering—the mechanism of fear turning into anger and blame follows a similar logic, as anger in the Star Wars saga is frequently caused by the blaming of others); *see also* HESIOD, THEOGONY 7-9 (M.L. West trans., 1999) (Uranos fears Kronos and his siblings and then blames the Titans for his fall, vowing revenge); David S. Rubenstein, *Immigration Blame*, 87 FORDHAM L. REV. 125, 143-167 (2018) (discussing how blame and blame-avoidance influence cognition and, in turn, policymaking).

in the run up to 9/11.[202] Concerns with responsibility and potential blame led to an under-sharing of critical information and thus culminated in a failure to respond to a national security threat that otherwise might have been forestalled.[203]

Tallinn 2.0 seeks to avoid this fault trap through its general diligence obligation.[204] States have an obligation to halt activity they know to cause significant adverse consequences internationally—even if the State did not itself perpetrate these actions.[205] It gives the State an out to deflect into action rather than into inaction. Further, *Tallinn 2.0* seeks to remedy willful blindness concerns by making States responsible for their constructive knowledge—that is, knowledge that a like-situated State would have had in similar circumstances.[206]

Tallinn 2.0's attempt to escape the fault trap, however, tends to lead right back into it. An example again helps illustrate this problem. In the week of December 16, 2019, the City of Frankfurt shut down its IT network.[207] The reason for the shutdown was the fear of a spread of an Emotet infection leading to ransomware attacks.[208]

Emotet is "an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans."[209] An Emotet infection is notoriously hard to detect because it "can evade typical signature-based detection."[210] It is further hard to remove from infected systems.[211] An Emotet infection spreads through malspam.[212] Importantly, Emotet can take over infected

---

202 *See* Amy Zegart, *In the Deepfake Era, Counterterrorism Is Harder*, THE ATLANTIC (Sept. 11, 2019), https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/ [https://perma.cc/3VDR-2ZHQ].

203 John A. Gentry, *Intelligence Failure Reframed*, 123 POL. SCI. Q. 247, 250 (2008).

204 TALLINN 2.0, *supra* note 22, at 30 r. 6.

205 TALLINN 2.0, *supra* note 22, at 40 r. 6 ¶ 36.

206 TALLINN 2.0, *supra* note 22, at 41 r. 6 ¶ 39.

207 Catalin Cimpanu, *Frankfurt shuts down IT network following Emotet infection*, ZDNET (Dec. 19, 2019), https://www.zdnet.com/article/frankfurt-shuts-down-it-network-following-emotet-infection/ [https://perma.cc/NTD3-V278].

208 *Id.*

209 *Alert (TA18-201A), Emotet Malware*, CISA (July 20, 2018), https://www.us-cert.gov/ncas/alerts/TA18-201A [https://perma.cc/S4BT-MACW].

210 *Id.*

211 *Id.*

212 *Id.*

machines and disseminate more malspam from infected accounts.[213] Emotet steals sensitive banking information from infected machines and has since morphed into a ransomware tool.[214]

The City of Frankfurt's actions were commendable in stopping the spread of a potentially dangerous cyber-infiltration by cyber criminals. Yet, had the City of Frankfurt (or the German government) conducted a *Tallinn 2.0* analysis, it might well have been dissuaded from acting. The consequence of acting is an admission by the City of Frankfurt that Emotet infections like the one it suffered are in fact detectable and, if left unaddressed, can lead to significant adverse consequences. In other words, it is an admission of knowledge and thus a trigger for a diligence obligation that the failure to abide is wrongful.[215]

This leads to a problem in its own right. Once knowledge is admitted, the diligence obligation vests.[216] It thus means that falling short of acting diligently from that point forward entails fault, and as such, liability.[217] Importantly, inaction would have had no such consequence: there was of yet no significant adverse consequence. The measure was preventive, and as such, a failure to take it would not have been wrongful under *Tallinn 2.0*.[218] That means that inaction is "free," and action potentially exposes an actor to liability. Anyone facing those consequences may well choose not to act out of precaution and thus avoid disaster.

This not the end of the problem: taking action once implies an obligation to take similar action again in the future or be subject to countermeasures. Now that one has taken action, one has constructive knowledge that future similar threats also will lead to significant adverse consequences.[219] Constructive knowledge implies that to act once creates an obligation to act again. Action, in

---

[213] *See generally Emotet computer virus spreading in Japan, Suga warns*, JPN. TIMES (Nov. 28, 2019), https://www.japantimes.co.jp/news/2019/11/28/national/emotet-computer-virus-spreading-japan-warns-official/#.XgPSby3Mx8c [https://perma.cc/AF57-X92J] (explaining that Emotet attaches to spoof emails, steals account information and sends out new fake emails).

[214] Emotet, MALWAREBYTES, https://www.malwarebytes.com/emotet [https://perma.cc/46AR-S4ZC] (last visited Dec. 25, 2019).

[215] TALLINN 2.0, *supra* note 22, at 40 r. 6 ¶ 37.

[216] TALLINN 2.0, *supra* note 22, at 40 r. 6 ¶ 37.

[217] *See generally* TALLINN 2.0, *supra* note 22, at 84 r. 14 (establishing that a State is internationally responsible for cyber acts that are attributable to that State).

[218] TALLINN 2.0, *supra* note 22, at 44-45 r. 7 ¶ 7.

[219] *See* TALLINN 2.0, *supra* note 22, at 41 r. 6 ¶ 39.

other words, appears to create a preventive duty for future cyber threats where none otherwise exists.[220] This again is far from ideal. It again, strictly speaking, would counsel to inaction rather than action.

The fault trap thus creates incentives not to govern *up*, in the sense of creating ever more sustainable governance structures that progressively improve cyber safety. To the contrary, the fault trap creates incentives to govern *down*, in the sense of acting only in a limited set of circumstances after a threat has already materialized to avoid future liability—or more pressingly, future lawful countermeasures. The fault trap is deeply destructive of good governance precisely because it creates no incentives to anticipate and coordinate positive responses.

One might object that if the City of Frankfurt had not acted, it certainly would have had to act in the aftermath of an Emotet attack. It would have been left to clean up the mess of the cyberattack. This may factually be true. Legally, however, the connectivity issue outlined in section III(a) makes sure that the City of Frankfurt could point to others as being at fault for any adverse consequences.[221] It could have pointed to vulnerabilities in recipients of City emails. It could blame operating systems. It could even seek to blame a third State for conducting a cyberattack against Germany. All of these strategies would deflect blame, undercut constructive knowledge, and lie fault at someone's else feet. A fault paradigm, in other words, is a horrible paradigm for any governance infrastructure to evolve and adapt to emergent threats. Given the fluidity of cyber in this respect, that is bad news for *Tallinn 2.0*.

d. Conclusion

Tallinn 2.0 seeks to do the right thing. It seeks to provide a legal matrix to guide decision-making in cyber. It does so on the basis of strong values embedded in general international law and an analysis of state practice. Yet, as this section has shown, its State- and fault-based approach has created significant issues for the accomplishment of its goals. Thus, *Tallinn 2.0* provides a roadmap not only for compliance but also for avoidance. And the roadmap

---

220 TALLINN 2.0, *supra* note 22, at 44-45 r. 7 ¶ 7.

221 *See supra* section III(a).

for avoidance is clearer (and cheaper) than the roadmap for compliance.

It may be that this is the best that can be done. No other translation may currently be possible. Bad incentives in general international law can be a good incentive to devise a better, treaty-based structure going forward.

As this Article outlines, a turn of the kaleidoscope might be able to place the *Tallinn 2.0* on stronger footing. This turn of the kaleidoscope would, at least in the soft sense, impose greater obligations on States. This makes it unlikely that States will shower it with praise.

And yet, it will have two advantages. First, for States, it also provides new partners with whom governance should become significantly more feasible—apex platform, apex programming, and apex infrastructure companies. Second, for international lawyers, it provides a better means to give legal force to international legal obligations, even in the absence of state-practice. It demonstrates that the application of a general principle of law can overcome the lack of positive consent to cyber norms. In this case, this more robust set of obligations may in fact prompt action to codify a more meaningful governance approach that would streamline the respective diligence obligations and governance structures to harness the promise of cyber.

IV. CYBER-COMMONS

The core proposal of this Article is to overcome the problems of the responsibility paradigm by replacing it with a commons paradigm. Such a commons paradigm would move away from a purely State-based approach to governance and allow additional actors to become core governance participants. It would also move away from a fault-based approach. Instead, it will focus on the concept of using—and of correlative rights to use—resources pooled in common between participants. This focus moves away from a logic of blame to a logic of coordination.

a. Defining Commons

Commons aggregate pooled resources. The classical example of a commons is a grazing pasture.[222] This grazing pasture does not belong to any one farmer.[223] It is either not owned at all or communally owned by those who use it. The concern of a commons is that overuse of the common pooled resource is unsustainable and eventually destroys the commons together with the resources it provided to its users. Classically, overgrazing destroys the pasture.[224]

This classical definition of commons sets up a stark contrast between resources that are privately owned and resources that are not owned (or communally owned) but commonly used. This dichotomy would suggest that commons principally refer to property (for example, land) and that this property is not owned by any one person: the grazing pasture is a commons because no one person owns the pasture. It is this conception that led the *Tallinn 2.0* experts to reject treating cyber as a commons.[225]

This classical definition does not do justice to commons or how common pool resources are held. The key example of a common pool resource that does not follow the dichotomy between private and communal ownership is water.[226] Water is a common pool resource because a large number of community members rely upon the same source of water in order to survive.[227] Water and particularly groundwater can be overused—that is to say, the overuse of groundwater leads to the eventual complete exhaustion or collapse of groundwater reservoirs.[228] Such a collapse would

---

222 *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1244 (1968).

223 *Id.*

224 *Id.*

225 TALLINN 2.0, *supra* note 22, at 12 r. 1 ¶ 5.

226 *See generally* Anne Hellum, *Engendering the Right to Water and Sanitation: Integrating the Experiences of Women and Girls*, *in* THE HUMAN RIGHT TO WATER: THEORY, PRACTICE AND PROSPECTS 300, 314 (Malcolm Langford & Anne Russell eds. 2017) (illustrating the integrated way in which poor African women use water for daily activities).

227 *Id.*

228 Dennis Dimick, *If You Think the Water Crisis Can't Get Worse, Wait Until the Aquifers Are Drained*, NAT'L GEOGRAPHIC (Aug. 21, 2014), https://www.nationalgeographic.com/news/2014/8/140819-groundwater-california-drought-aquifers-hidden-crisis/ [https://perma.cc/AS5A-RKX2].

deprive all users of future water access. In this sense, groundwater access is like access to a grazing pasture.[229]

Groundwater access is *unlike* access to a grazing pasture in an important respect: the communities and farmers using the groundwater have a potentially enforceable property right in the water they use.[230] The problem is that they hold *inconsistent* rights.[231] This inconsistency could lead to the ejection—and thus loss of rights—by a large swath of water right holders.[232] This is a consequence that is so destructive of communities relying upon groundwater that it is unfathomable to impose.[233] Alternatively, it can act as an accelerant to insisting on one's right and could hasten the destruction of the groundwater reservoir; every rights holder would increase use so as not to admit that prior use was impermissible, thus hastening the demise of the commons.[234]

This story of groundwater as a commons is the story of water in Southern California. As Elinor Ostrom's classical *Governing the Commons* outlines, communities in Southern California fought over use of the same groundwater basins.[235] California law, through the reasonable use and correlative rights doctrines, in principle, would have provided a means to resolve this legal dispute.[236] Yet, the reasonable use doctrine led to precisely the kind of disincentives that might cause reservoirs to collapse because timing litigation right was too treacherous to yield meaningful results.[237] Negotiating to a reasonable use of a common pooled resource—and treating the reservoir as a commons—was the far more efficient solution.[238]

Ostrom provides yet another water-based example of a commons—namely, access to water in the *Zanjera* in the

---

229 *See* Burke W. Griggs, *Beyond Drought: Water Rights in the Age of Permanent Depletion*, 62 U. KAN. L. REV. 1263, 1300 (2014).

230 *See id.*

231 *See id.* at 1299-1300.

232 *See id.* at 1302.

233 *Id.*

234 *See generally* OSTROM, *supra* note 32, at 104-110 (examining several institutions to manage groundwater basins located beneath Los Angeles).

235 *Id. See also* Griggs, *supra* note 229.

236 Burke W. Griggs & James J. Butler, Jr., *Groundwater in the American West: How to Harness Hydrogeological Analysis to Improve Groundwater Management*, *in* THE WATER PROBLEM, CLIMATE CHANGE AND WATER POLICY IN THE UNITED STATES 113, 120 (Pat Mulroy ed., 2017).

237 *See* OSTROM, *supra* note 32, at 114.

238 OSTROM, *supra* note 32, at 108-10.

Philippines.[239] *Zanjeras* are common irrigation works used to bring water to farmland.[240] Tenant farmers in particular were able to exchange their labor in building these irrigation works for non-irrigated land for tenancy rights in newly irrigated parcels.[241] The irrigation works are communally maintained.[242] Water-allocation typically does not create problems so long as the irrigation works are maintained.[243] Yet, in droughts, water rights are by rotation, and the closing of canals is communally guarded and enforced.[244]

b. Cyber as Commons

Treating cyber as a commons is not a new idea. A significant literature has developed to treat cyber as a commons.[245] Much of this literature, as discussed in *Tallinn 2.0* itself, analogizes cyber to the deep sea.[246] It therefore submits that cyber should be treated as owned in common.[247]

This is not the only way to treat cyber as a commons. Rather, one can treat cyber as a commons in the sense of water rights. Thus, as in the context of water rights, cyber is certainly anchored in property rights to be part of the cyber stream. As *Tallinn 2.0* points out, cyber infrastructure is physical and under the territorial jurisdiction of States.[248] In the same way, in the water context, there is physical infrastructure linking a parcel of land to water.[249] Further, in both contexts, this infrastructure implies a right to the use of a flow of the common pooled resource. In the water context,

---

239 OSTROM, *supra* note 32, at 82.

240 OSTROM, *supra* note 32, at 82-83.

241 OSTROM, *supra* note 32, at 82.

242 *See* OSTROM, *supra* note 32, at 82-86.

243 *See* OSTROM, *supra* note 32, at 86-87.

244 OSTROM, *supra* note 32, at 67.

245 *See generally, e.g.*, Shackelford, *supra* note 32, at 29-37 (analogizing global commons regimes to cyber); *see also* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 509-18 (2003) (discussing the undesirable development of cyberspace away from a commons akin to a grazing pasture towards an anti-commons defined by property rights); Sean Watts & Theodore Richards, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 771, 779-91 (2018) (critiquing the commons literature).

246 TALLIN 2.0, *supra* note 22, at 12 r. 1 ¶ 5.

247 *See* sources cited *supra* note 245.

248 TALLIN 2.0, *supra* note 22, at 12 r. 1 ¶ 5.

249 *See* OSTROM, *supra* note 32, at 82-87.

the flow is access to a flow of ground water or flow from the irrigation system when one's turn in the rotation arrived.[250] In the cyber context, the right is one to access to connectivity and information.

Despite these property rights anchoring cyber in public and/or private ownership, cyber remains a commons in two respects. *First*, what gives cyber value is precisely that it is a shared resource. The point of cyber, its very definition, is global connectivity.[251] *Second*, cyber only works if it is diligently maintained by all of the global participants.[252]

In both respects, cyber is like the *Zanjeras* in the water context.[253] If the irrigation works are not maintained, the *Zanjera* farmers do not receive access to water.[254] This means that the *Zanjera* farmers rely upon others doing their part in maintaining irrigation works in order to receive the benefit they seek.[255]

This is also the case in the cyber context. In order to have the benefit of the cyberspace we expect every time we go online, the entire global cyber-infrastructure must be maintained and kept in good repair.[256] This means that every daily user of cyber, much like

---

250 *See* OSTROM, *supra* note 32, at 86-87.

251 *See* Jennifer Bussell, *Cyberspace*, ENC. BRITANNICA (Mar. 12, 2013), https://www.britannica.com/topic/cyberspace [https://perma.cc/3B7D-LVCP].

252 *See id;* Adrian Booth et al., *Critical infrastructure companies and the global cybersecurity threat*, MCKINSEY (April 11, 2019), https://www.mckinsey.com/business-functions/risk/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat# [https://perma.cc/G2XA-XQEK] (detailing the need for global cyber-security approaches and the danger of collateral damages from nonspecific attacks globally).

253 *See generally* OSTROM, *supra* note 32, at 82-7 (explaining the way *Zanjeras* work).

254 OSTROM, *supra* note 32, at 82-7

255 OSTROM, *supra* note 32, at 82-7

256 *See generally* Elena Chernenko, Oleg Demidov & Fyodor Lukyanov, *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*, COUNCIL ON FOREIGN REL. (Feb. 23, 2018), https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms [https://perma.cc/7YF4-MNXK] (examining the emergent problems of cyber threats and inviting cooperation between States to tackle the problem in the future); Ankit Fadia, Mahir Nayfeh & John Noble, *Follow the leaders: How governments can combat intensifying cybersecurity risks*, MCKINSEY (Sept. 16, 2020), https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks [https://perma.cc/ULP5-RNWW] ("Any attack on critical infrastructure in one sector of a country can lead to disruption in other sectors as well. An attack on a country's telecommunications, for example, may disrupt

the *Zanjera* farmer, relies upon the work of others beyond his or her own control to make sure those crucial flows reach him or her. And every State relies upon the work of other States and other platforms, protocols, and operating systems.[257] Cyber only works together.

Cyber is a common pooled resource, and cyberspace is a commons because no one person, or even one group of persons, can build cyberspace alone. Imagine building Instagram with only your high school friends, LinkedIn with only your current work colleagues, and TikTok with only your law school classmates. Imagine an internet without PayPal, eBay, Amazon, or Google. Imagine a moot court competition or law journal symposium without Westlaw, interactive maps, or UberEats. It is not the same thing. And you do not have to imagine this. All you have to do is ask—is the carefully curated internet in the People's Republic of China or the Democratic People's Republic of Korea *the internet*?[258] And are people in the People's Republics the better off for the curating? Just look at the streets of Hong Kong, and you will have the answer.[259]

c. Governing the Commons

This leaves the question of how to govern cyber as a commons. The remainder of this Article will outline such an approach based on a general nuisance principle. Before launching into that discussion, however, a few guideposts from the commons literature are needed to guide the discussion.

---

electronic payments. But this is just part of the problem" because of the global impact of such threats on "an estimated 127 new devices connect[ed] to the internet every second [globally]. Any disruption in digital connectivity is considered an obstacle in the path of progress . . . .").

257 *See* Chernenko, Demidov & Lukyanov, *supra* note 256.

258 *See generally China, North Korea among 10 countries cited for extreme media censorship: Watchdog*, STRAITS TIMES (Sept. 10, 2019), https://www.straitstimes.com/world/china-north-korea-among-10-countries-cited-for-extreme-media-censorship-watchdog [https://perma.cc/CJJ6-G738] (regarding internet censorship in China, North Korea, and other countries).

259 *See* Jeremy Hsu, *Fear of Internet Censorship Hangs Over Hong Kong Protests*, IEEE SPECTRUM (Nov. 22, 2019), https://spectrum.ieee.org/tech-talk/telecom/internet/fear-of-internet-censorship-hangs-over-hong-kong-protests [https://perma.cc/6RJT-3S44] (discussing the links between growing internet censorship and the Hong Kong protests).

The first point concerns the role of law. Law can function as a set of textual rules to apply in a court-like setting.[260] Criminal law might function much in this way. But cyber is not a domain where law could be applied with such a precision due to the lack of state practice and normative consensus on cyber questions.[261] Rather, law is a tool to guide decision-making rather than to compel it.[262]

This feature of law is amplified in the commons governance context. The California groundwater commons example is instructive.[263] The courts in that context were inadequate to resolve the growing commons crisis on their own.[264] Litigation was too slow, too expensive, and ultimately too unpredictable to serve as a cure-all for the groundwater crisis.[265] Rather, commons governance came as a negotiated agreement, negotiated bit by bit in a trust building exercise.[266]

But to conclude that law—and courts—had no role to play would significantly underestimate the role of law in commons governance. Quite to the contrary, law and legal processes supported decision-making at every step of the way by framing the question in terms of equitable use.[267] Further, the courts provided a means to enforce negotiated agreements as consent decrees.[268] Law was thus instrumental in bringing commons governance to a successful outcome by empowering commons actors to communicate with each other in an idiom capable of reaching common ground and sustainable solutions.

The California story already hints at another feature of commons governance: it takes all kinds of actors to make it work.[269] This approach to governance drawing in public and private actors and hybrid institutions combining both private and public functions is known as "polycentric" governance.[270] The term "polycentric" governance describes an arrangement which "[i]nstead of relying strictly on hierarchical relations, as within a single firm . . . is

---

260 REISMAN, *supra* note 152152, at 177-83.

261 *See* section II.

262 REISMAN, *supra* note 152152, at 183-194.

263 OSTROM, *supra* note 32, at 103-42.

264 OSTROM, *supra* note 32, at 114.

265 OSTROM, *supra* note 32, at 114.

266 OSTROM, *supra* note 32, at 114.

267 OSTROM, *supra* note 32, at 103-42.

268 OSTROM, *supra* note 32, at 119-23.

269 OSTROM, *supra* note 32, at 133-36.

270 Shackelford, *supra* note 32, at 7-9.

governed by negotiation and bargaining processes among many different actors in several different arenas."[271] These processes, in turn, interact with each other to diffuse the ultimate decision-making authority from a single place of central power to the entire network of participants.[272]

As this description already suggests, it is a governance model that can be and has been applied to cyber. It has been applied to a discussion of cyber security.[273] Similar structures are in place to govern the development of internet code itself.[274] Commons governance, in other words, is already part and parcel of cyber governance regimes even if the legal processes needed to support them remain in shadow.

A key to the success of polycentric governance is to move away from fault and towards cooperative trust-building. The point of commons governance is not to blame someone when something has gone wrong. It is to prevent things from going wrong in the first place. For this reason, commons governance is particularly successful when infraction rates are low and punishment of infractions is not draconian but graduated, and thus not the principal deterrent.[275] Rather, the principal deterrent from infracting is the violation of trust—and inherent threat of loss of one's own share of the common pooled resource.[276]

This feature of commons governance has two key takeaways for the law needed to support it. First, the law, too, must move away from a fault-based approach and create a language in which shared use can take over as the principal governance paradigm. Law must facilitate rather than prohibit, communicate rather than command, support rather than judge, for commons governance to succeed. And it must remain flexible when called upon to actually resolve a dispute, so as not to disincentivize future shared use by over-punishing infractions in its own right, and thereby contributing to an erosion of trust and continued cooperation.

Second, trust is good. Trust-but-verify is better. Successful commons governance approaches always involve a form of mutual

---

271 OSTROM, *supra* note 32, at 135.

272 OSTROM DIVERSITY, *supra* note 32, at 281-86.

273 Shackelford, *supra* note 32, at 6-26.

274 GRALF-PETER CALLIESS & PEER ZUMBANSEN, ROUGH CONSENSUS AND RUNNING CODE: A THEORY OF TRANSNATIONAL PRIVATE LAW 134-39 (2010).

275 OSTROM, *supra* note 32, at 94-100.

276 OSTROM, *supra* note 32, at 94-100.

monitoring.[277] And this mutual monitoring is the most successful when it is done by people interacting with each other on a frequent and close basis.[278] Neighbors watching neighbors is a powerful incentive to act consistently with neighborhood standards for all involved.[279] Such monitoring works because the person monitoring will herself have to live with the rules she applies to others—the person monitoring will in turn be monitored by the very people he or she called out for an infraction. But if a person respected for "walking the walk" in the community could call out a person for an infraction, the loss of communal standing is a powerful disincentive for defecting from the commons governance paradigm in the first place.

This second takeaway from commons governance suggests that the law should always look to build communities that in turn will help to govern up. Neighbors should monitor neighbors. But they should do so not to gain a petty advantage that hurts the commons in the long run and thus govern down. They should do so in a manner that protects the sustainability of shared use. The way to achieve this second goal is again to look to polycentricity. A hierarchical system can reward "collaborators" who seek personal gain to the detriment of the common good. A polycentric governance process that subjects all to reciprocal obligations and enforcement is less susceptible to such incentives.

V. CYBER-NUISANCE

This Article proposes that the best way to institute a commons-based paradigm of cyber governance is to embed a principle of cyber nuisance in cyber governance decision-making. This part first defines what general principles are in section A. Section B then establishes the existence of such a nuisance principle for governance of correlative rights. Section C subsequently discusses how this principle would function in the cyber context.

---

277 OSTROM, *supra* note 32, at 94-100.

278 OSTROM, *supra* note 32, at 94-100.

279 OSTROM, *supra* note 32, at 94-100.

a. A Return to Principles

General principles are an overlooked source of international law. The discussion in Tallinn 2.0 focuses on customary international law, application of international treaty norms by analogy, and the translation of potentially applicable international law norms drawn from other areas of international law.[280] Yet, it reasonably neglects general principles of law.

This neglect is understandable to a point. General principles of law are frequently treated with mild derision by international law academics. One went as far as suggesting that general principles are nothing but platitudes translated to Latin.[281] Further, general principles of law are reasonably far away from "positive" expressions of the will of State on the international stage. To use them therefore has an air of unwelcome natural law indulgence.[282]

That being said, general principles of law formally are co-equal sources of international law alongside treaties and custom.[283] They were included in the source of international law precisely to deal with situations in which no existing customary rule or treaty rule clearly resolves a given problem.[284] The point of general principles is to provide means to avoid a conclusion that there is no international law governing a particular problem.[285] As this is precisely the situation in which cyber currently finds itself, it would be prudent, given the structure of the sources of international law, to consult them.

The snark-filled remark that general principles of law are platitudes turned Latin similarly should be no reason to ignore them.[286] It is certainly true that many general principles have Latin names.[287] It is similarly true that many of them appear to express platitudes (think *ex iniuria non oritur ius*—which flippantly could be

---

280 TALLINN 2.0, *supra* note 22, at 12 r. 1 ¶ 5.

281 OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 54 (1991).

282 BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 3-4, 19 (Cambridge Univ. Press 2006).

283 Statute of the International Court of Justice, art. 38 § (1)(c), June 26, 1945, 59 Stat. 1051, 33 U.N.T.S. 993.

284 HERSCH LAUTERPACHT, THE FUNCTION OF LAW IN THE INTERNATIONAL COMMUNITY 93 (rev. ed. 2011).

285 *Id.*

286 SCHACHTER, *supra* note 281281.

287 CHENG, *supra* note 282, *passim*.

translated as "a wrong can't make a right").[288] But that does not mean that these principles are not helpful in a pinch. Just think how many times sophisticated lawyers refer to estoppel and "a wrong can't make a right" will appear somewhat less absurd a proposition to rely upon in legal argument.[289]

That is not to say that the proof of a general principles is always easy. Quite to the contrary, it is treacherous. Proof of a general principle requires one to establish that a representative set of relevant legal systems would address a core problem in a similar way.[290] This means that it is not enough to look in a Restatement or Code. Some legal systems have the exact same rule—sometimes verbatim—on the books but apply them differently.[291] Others do not appear to have the same rule on the books at all but reach similar results in practice all the same.[292] One therefore has to examine how the law works in practice. The method to do so is known as functional legal comparison.[293] And it is by far the best suited to establish a general principle.

The benefit of general principles of law established on the basis of functional legal comparison is that they can find application beyond international law. General principles of law established on the basis of functional comparison also form part and parcel of transnational law.[294] Transnational law is, at a minimum, a material source of law for global business transactions.[295] Principles drawn from transnational law are habitually applied in international commercial arbitration.[296]

---

288 CHENG, *supra* note 282, at 187.

289 T. Leigh Anenson, *The Triumph of Equity: Equitable Estoppel in Modern Litigation*, 27 REV. LITIG. 377, 439-40 (2008).

290 For a full discussion, see Frédéric Gilles Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345, 367-75 (2017) [hereinafter Sourgens, *Privacy*]; Michael D. Nolan & Frédéric Gilles Sourgens, *Issues of Proof of General Principles of Law in International Arbitration*, 3 WORLD ARB. & MEDIATION REV. 505, 509-10 (2009).

291 Rodolfo Sacco, *Legal Formants: A Dynamic Approach to Comparative Law I*, 39 AM. J. COMP. L. 1, 24 (1991).

292 Sourgens, *Privacy*, *supra* note 290290, at 371.

293 Ralf Michaels, *The Functional Method of Comparative Law*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 339, 342 (Mathias Reimann & Reinhard Zimmermann eds., 2006); KONRAD ZWEIGERT & HEIN KÖTZ, EINFÜHRUNG IN DIE RECHTSVERGLEICHUNG 15-31 (3d ed. 1998).

294 *See* Emmanuel Gaillard, *Transnational Law: A Legal System or a Method of Decision Making?*, 17 ARB. INT'L 59, 62 (2011).

295 *Id.*

296 *See* Nolan & Sourgens, *supra* note 290290.

A great deal of transactions related to cyber governance are currently resolved in international commercial arbitration.[297] These proceedings, too, frequently rely upon a kind of transnational law. Fitting existing stereotypes, this particular field of transnational law gave itself a Latin name—the *lex digitalis*.[298]

A general principle of law on cyber security drawn from private law stands a good chance to integrate both into public international law and the amorphous world of the *lex digitalis*. It thus would be a candidate that could live up to the promise of commons governance through polycentricity. Or, to put it in English, it would have the benefit of coordinating State-based and non-State based global approaches to cyber governance and thus would be able to build a legal bridge where one is sorely needed.

So far, the appeal to general principles underlying this Article has been largely formal: general principles are a formal source of international law and a material source of transnational law, so we should consult them. One therefore might ask: why is it a good idea functionally to consider general principles? To answer this question, consider why one looks for a legal decision-making matrix as opposed to, say, an ideological one. The premise of this Article has been that lawless spaces are inherently undesirable and that one should strive to provide legal tools for decision-making no matter what. It is in good company in doing so.[299]

The reason for this insistence is that law does a particularly good job, all things considered, to weigh conflicting values and balance countervailing interests in an even-handed and predictable manner.[300] While legal solutions may not always be fair, they are always identifiably similar in the way they resolve value conflicts.[301] Or, to put this in more practical terms, one will always know when "the lawyers got involved" even if one does not know the law of a particular jurisdiction.

The reason to appeal to general principles is that general principles help draw up a kind of grammar or map for legal

---

[297] *See ICANN Programs*, INT'L CENT. FOR DISP. RESOL. (2021), https://www.icdr.org/icann [https://perma.cc/ZMT2-FGXK].

[298] Ralf Michaels, *Global Legal Pluralism*, 5 AN. REV. L. & SOC. SCI. 243, 247 (2009) [hereinafter Michaels, *Pluralis*m].

[299] REISMAN, *supra* note 152152, at 21; LAUTERPACHT, *supra* note 284284, at 93.

[300] *See* REISMAN, *supra* note 152152, at 185 (noting the need for an eclectic legal method).

[301] *See* REISMAN, *supra* note 152152, at 185.

decision-making in general.[302] They show what kind of values are involved and how these values could be balanced against each other. The fact that disparate legal systems arrive at a broadly similar way of balancing value conflicts is helpful no matter the formal force of general principles in their own right. It suggests that to weigh differently risks losing sight of, or underplays, a value otherwise held in higher regard by legal decision-making.[303] Any such cognitive dissonance in the law (or dare one say, false consciousness) should give one pause whether a particular prescription is chosen for its expedience to resolve a particular problem in one's perceived favor.[304] In short, if one strives to uphold the rule of law, one should take law seriously. Disregarding general principles is a poor way to do so.

This leaves the question which legal system to examine. Space constraints—or more to the point, the attention span of the reader—counsel against a universal comparative exercise. This Article, and the project of which it forms a part, suggest that one way to narrow down the legal systems to include in a study is to look to States that have a particular role to play in cyber and cyber operations.[305] If these States hail from diverse legal systems and socio-economic experience, the choice would have both relevance to the problem to be solved (how do I convince a lawyer from X that what we are doing is wrong?) and represent the significant diversity of legal systems of the world. This Article therefore has chosen to examine the laws of the United States, France, the Russian Federation, the People's Republic of China, Israel, and *shari'a*.

This formally leaves two continents out of the study: much of Africa and South America. As there is no State that would easily fit the criteria chosen to pick legal systems, the Article has chosen not to study a specific jurisdiction from these continents in their own right. It will, however, note where representative jurisdictions from these continents follow a similar path to resolving the underlying problem while keeping an eye on the jurisdictions which, for good or ill, are most closely aligned with cyber operations and thus most

---

302 *See* REISMAN, *supra* note 152152, at 190-94 (discussing the task of map-making in international law).

303 *See* REISMAN, *supra* note 152152, at 185.

304 Claire A. Hill, *Cheap Sentiment*, 81 LAW & CONTEMP. PROBS. 67, 69-75 (2018); Mark G. Yudof, *'Tea at the Palaz of Hoon': The Human Voice in Legal Rules*, 66 TEX. L. REV. 589, 620-21 (1988).

305 Sourgens, *Privacy*, *supra* note 290290, at 375-78.

immediately are called upon to step up their involvement in global cyber governance.

b. Nuisance, Correlative Rights, and Cyber-Governance

The concept of commons governance is firmly established in all of the legal systems studied. What is more, the concept of commons governance follows broadly on what common lawyers would consider the logic of nuisance. The nuisance principle—as it develops in this section—looks to restrain unreasonable overuse through a protection of correlative rights. It does so without falling into a fault-based paradigm. It further provides carefully calibrated incentives to cooperate in use and respect the reasonable correlative rights of one's neighbors. In short, nuisance is a principle that meets the requirements of commons governance well.

The key to nuisance is that it is not only a principle that can guide decision-making, though it is that too.[306] It is also a principle that can lead to the assertion of a cause of action.[307] Thus, it is not just a means to think about factors impacting decision-making, it is also a means to police this decision-making at the margins. It thus provides an additional incentive for decision makers to act in a manner consistent with the sustainability of the commons as a failure to do so could, in the right circumstances, become actionable.

Nuisance finally exhibits key features to support polycentric governance.[308] As discussed below, nuisance and correlative rights always look to neighborhood standards in one form or another. The first imperative of nuisance is common use protection, the enforcement of correlative rights. But precisely how this imperative is met is defined by context as the rights of each are correlative to those of the others in the commons. Nuisance, in other words, respects and enforces the self-regulatory equilibria reached in a particular community. It does not seek to displace them.

Further, nuisance as a general principle has the benefit of being seamlessly enforceable. A principle of cyber-nuisance would be a general principle of international law. As such, it is a principle that

---

306 *See* REISMAN, *supra* note 152, at 183-90 (discussing the contextual-policy based mode of international law).

307 *See* Crosstex N. Tex. Pipeline, L.P. v. Gardiner, 505 S.W.3d 580, 588, 605, 607 (Tex. 2016); Trail Smelter Arbitration (U.S. v. Canada) 1938/1941, R.I.A.A. 1905.

308 *See* OSTROM DIVERSITY, *supra* note 32, at 281-86.

should govern the decision-making of States.[309] But it is more than just a general principle of international law. It is also a general principle of transnational law—that is, a general principle of private law that is enforceable in international commerce.[310] This, too, supports the polycentric nature of commons governance.[311] Rather than capturing only a principle exclusive to State concerns in cyber, the same principle also guides corporate concerns. Given the power of apex platforms, operating systems, and infrastructure companies, this expansion of the scope of application of the principle means that these actors are finally brought into the fold. Not only that, but a failure by these actors to take commons concerns into consideration in making their own business decisions would provide a ready cause of action—and not just for the business partners of these companies in transnational commerce. Rather, cyber-nuisance, once fully adopted, provides a ready domestic means for affected parties to cause compliance by private actors no matter where they might be located.

i. United States

Restatement (Second) of Torts is the classic statement of nuisance law in the United States.[312] The Restatement distinguishes between private and public nuisance.[313] The Restatement defines a private nuisance as conduct, whether intentional and unreasonable or otherwise negligent, reckless, or abnormally dangerous, which legally causes the invasion of another's interest in land.[314] A nuisance can arise out of either an action or an omission.[315] The Restatement provides that a failure to act constitutes a nuisance if there is some positive duty to "prevent or abate the interference with the public interest or the invasion of the private interest."[316]

---

309 LAUTERPACHT, *supra* note 284284, at 93.

310 KLAUS PETER BERGER, THE CREEPING CODIFICATION OF THE NEW LEX MERCATORIA 202 (2d ed. 2010).

311 OSTROM DIVERSITY, *supra* note 32, at 281-86.

312 RESTATEMENT (SECOND) OF TORTS (AM. LAW. INST. 1979). I will refer to it as the "Restatement" in the text from here on out for ease of reference.

313 *Id.* at § 821.

314 *Id.* at § 822.

315 *Id.* at § 824.

316 *Id.* at § 824(b).

The Restatement further treats as intentional an interference or invasion, which the perpetrator "knows [will result] or is substantially certain to result from his conduct."[317] To constitute a nuisance, such intentional interference or invasion must be "unreasonable."[318] To determine if it is unreasonable, the Restatement weighs the gravity of the harm against the utility of the conduct, looking to the respective social benefits of the interests involved and the extent and character of the harm and conduct.[319]

The Restatement defines a public nuisance as "an unreasonable interference with a right common to the general public."[320] The Restatement explains in the comments that "[a] public right is one common to all members of the general public" and that the right "is collective in nature and not like the individual right that everyone has not to be assaulted or defamed or defrauded or negligently injured."[321] The Restatement cites water pollution as a key example of such a public right.[322] The Restatement then again uses a multifactor test to weigh whether the interference with the public right is unreasonable.[323] Importantly, these factors look to public safety and public peace.[324] They further consider "whether the conduct is of a continuing nature or has produced a permanent or long-lasting effect, and, as the actor knows or has reason to know, has a significant effect upon the public right."[325]

So far, the Restatement approach to private nuisance at least appears to take a fault-based approach. That is, the Restatement suggests that one must prove either negligence (and as such tortious in its own right) or intentional endangerment.[326] This impression however is misleading.

Particularly, as a brilliant study by Professor Jill Fraley has shown, state courts do not follow this tort-based approach to nuisance but rather anchor nuisance in property law and the right

---

317 *Id.* at § 825(b).
318 *Id.* 312at § 822.
319 *Id.* at §§ 826-28.
320 *Id.* at § 821B.
321 *Id.* at § 821B, cmt. g.
322 *Id.*
323 *Id.* at § 821B(2).
324 *Id.* 312at § 821B(2)(a).
325 *Id.* at § 821B(2)(c).
326 *Id.* at § 822.

to exclude.[327] As Professor Fraley explains, "few courts have adopted this switch in the intent requirement for nuisance."[328] Instead, "a larger number of states by far maintain the traditional position, which extends liability for nuisance beyond acts that are intentional or negligent to interferences more generally, regardless of the conduct of the defendant."[329]

What Professor Fraley correctly recognizes is that nuisance critically goes to the right to exclude others from property.[330] From a property perspective, nuisance is a claim which lies for the unreasonable interference with enjoyment of property rights that is not a trespass.[331] The key to understanding this dominant understanding of nuisance in the courts is that liability is not strict—rather, it focuses on the reasonableness of the interference.[332]

To put another way, nuisance properly construed is a claim that lies in the context of the undue interference with correlative rights.[333] Correlative rights exist when multiple people have rights to a common pool resource.[334] These correlative rights are negative rights: they impose a duty on each user of the common pool resource to act so as not to destroy the entitlement of another user.[335]

---

[327] *See* Jill M. Fraley, *Liability for Unintentional Nuisances: How the Restatement of Torts Almost Negligently Killed the Right to Exclude in Property Law*, 121 W. VA. L. REV. 419, 451 (2018) ("[N]uisance is quintessentially about property, not about tort. The primary function of nuisance law is to limit the normally rather unlimited freedom that a property owner has to use her land as she likes.").

[328] *Id.* at 421.

[329] *Id.* at 422.

[330] *Id.* at 423.

[331] *Id.* at 453; Henry E. Smith, *Exclusion and Property in the Law of Nuisance*, 90 VA. L. REV. 965, 992-6 (2004).

[332] *See* Fraley, *supra* note 327, at 456 ("Subsets of nuisance law were strict . . . . Outside those subsets, however, nuisance law was not unlimited."); *see also* Smith, *supra* note 331, at 992 ("Under more modern approaches to nuisance, balancing tests are often invoked at the liability or remedy stage").

[333] *See* Bradford W. Wyche, *A Guide to the Common Law of Nuisance in South Carolina*, 45 S.C.L. REV. 337, 357 (1994) ("Similarly, in Young v. Brown, the court stated that 'due regard must be had to the correlative rights of the parties' in determining whether an activity should be declared a private nuisance" (quoting 212 S.C. 156, 169 (1948)); *but see* Tara K. Righetti, *Correlative Rights and Limited Common Property in the Pore Space: A Response to the Challenge of Subsurface Trespass in Carbon Capture and Sequestration*, 47 ENVTL. L. REP. NEWS & ANALYSIS 10420, 10431-32 (2017) (discussing the dangers of watering down trespass with a Restatement version of nuisance).

[334] Pierce, *supra* note 36, at 245-46.

[335] Pierce, *supra* note 36, at 246.

But correlative rights also give users a positive right to access and enjoyment of the common pool resource.[336]

One common example of correlative rights is the situation in which multiple lessees produce oil and gas under multiple distinct leases from a single formation.[337] Correlative rights here have two parts: (1) the right to produce from, and duty to preserve, the integrity of the reservoir; and (2) the right to, and duty not to interfere with, a reasonable portion of the common pooled resource.[338]

The interference with a correlative right could be actionable in trespass.[339] Yet, this trespass logic has been receding.[340] Rather, the focus more appropriately is on the loss of one's own right to use by another's use of the correlative share of a common pool resource.[341]

This focus now again sounds peculiarly like nuisance construed as a property law concept. The interference with correlative rights frequently is not a trespass for the reasons outlined by Professor David Pierce in his seminal work on oil and gas rights.[342] This leaves the question whether it is an actionable infringement of the right to a common pooled resource under the second string of "trespass or nuisance."[343] The main objection developed to such a classification advanced by Professor Pierce is that "nuisance is a tort remedy to protect property; it does not define the property itself."[344] Correlative rights, on the other hand, do so define the property.[345] This much of course is true.

---

336 Pierce, *supra* note 36, at 246.

337 Pierce, *supra* note 36, at 246, 253-255.

338 Pierce, *supra* note 36, at 256.

339 Pierce, *supra* note 36, at 259-64.

340 *See, e.g.*, Coastal Oil & Gas Corp. v. Garza Energy Trust, 268 S.W.3d 1, 4 (Tex. 2008) (holding "the rule of capture bars recovery" of any damages that may have been available under a trespass approach). For a discussion of the case, see Theresa D. Poindexter, *Correlative Rights Doctrine, Not the Rule of Capture, Provides Correct Analysis for Resolving Hydraulic Fracturing Cases [Coastal Oil & Gas Corp. v. Garza Energy Trust, 268 S.W.3d 1 (Tex. 2008)]*, 48 WASHBURN L.J. 755, 756 (2009) ("By failing to analyze trespass, the court did not properly apply the rule of capture").

341 Pierce, *supra* note 36, at 259-64.

342 Pierce, *supra* note 36, at 259-64.

343 Colleen E. Lamarre, *Owning the Center of the Earth: Hydraulic Fracturing and Subsurface Trespass in the Marcellus Shale Region*, 21 CORNELL J.L. PUB. POL'Y 457, 478-79 (2011) (discussing Jameson v. Ethyl Corp., 609 S.W.2d 346, 351 (Ark. 1980)).

344 David E. Pierce, *Minimizing the Environmental Impact of Oil and Gas Development by Maximizing Production Conservation*, 85 N.D. L. REV. 759, 768 (2009).

345 *Id.*

The point remains however that the *interference* with the right to access a commons, once that right has been defined, is a nuisance. If there is no right without a remedy, nuisance thus has a significant role to play in defining correlative rights.[346] This is so in jurisdictions that do not follow Restatement, as Fraley has correctly explained.[347] In those jurisdictions, nuisance has begun balancing the relative rights of users against each other and thus to bring in force the best approximation of their reasonable use rights from the common pool resource.[348]

Even in jurisdictions like Texas that more closely follow the Restatement approach, however, Professor Pierce's observation makes the substantial interference with a correlative right remediable as a nuisance. Per *Crosstex North Texas Pipeline, L.P. v. Gardiner*, nuisance at Texas law is a "legal injury involving interference with the use and enjoyment of real property."[349] *Crosstex* further established that the interference must be substantial to rise to the level of a nuisance.[350] The cause of action to recover for such nuisance in Texas requires showing of intent (intent to harm or substantial certainty of harm) or negligence (duty, breach, causation, harm).[351] The allegation that a person violated correlative rights provides the predicate for such a claim: correlative rights are negative rights and create a legal duty the breach of which would satisfy the negligence prong.[352] If the breach causes substantial interference with the enjoyment of correlative rights, it can thus be remedied as a nuisance. This correlative right cause of action seeking to remedy a nuisance then even under Texas law returns to its property roots: it could benefit from an injunction as opposed to mere money damages.[353]

This distinction between trespass and nuisance makes a difference. Another Texas case currently making waves, *Lightning*

---

346 Doug Rendleman, *The Triumph of Equity Revisited: The Stages of Equitable Discretion*, 15 NEV. L.J. 1397, 1426 (2015) ("The Supreme Court has not been completely faithful to no right without a remedy.").

347 Fraley, *supra* note 327, at 423.

348 Fraley, *supra* note 327, at 457-58.

349 *Crosstex*, 505 S.W.3d at 588.

350 *Id.* at 595.

351 *Id.* at 605, 607.

352 Pierce, *supra* note 36, at 245-46.

353 *Crosstex*, 505 S.W.3d at 610.

Oil v. Anadarko E&P Offshore, illustrates why.[354] The case involved facts typically seen only on a Property law exam: Lightning Oil held a lease to produce oil and gas from the owner of the relevant mineral estate.[355] Anadarko meanwhile sought and received the right from the surface owner to drill across the land to access minerals adjacent to Lightning's lease.[356] Lightning Oil objected to Anadarko's activity as inconsistent with Lightning Oil's rights under the lease.[357] Anadarko offered to move its drill site and Lightning Oil made clear that it would object to *any* drilling activity by Anadarko.[358] Lightning Oil eventually claimed for trespass and tortious interference with contract.[359]

The Texas Supreme Court rejected both claims.[360] In focusing its analysis on the relationship of the surface estate and the mineral estate, the court placed them in a position that eerily looks like correlative rights.[361] Then comes the key passage: "an unauthorized interference with the *place* where the minerals are located constitutes a trespass as to the mineral estate only if the interference infringes on the mineral lessee's ability to exercise its rights."[362] In context, this is no longer a trespass. The *Lightning Oil* court treated the question as one of nuisance akin to *Crosstex*—it required a non-trifling interference with the *exercise*, that is, enjoyment, of a right as opposed to any infringement of an absolute right.[363] Finding no interference with the *use* right, the *Lightning* court dismissed.[364] To predict future holdings post-*Lightning*, the correlative rights and nuisance approach is more likely to hit on the concerns raised in *Lightning* than the trespass jurisprudence would: to satisfy Texas

---

354 Lightning Oil Co. v. Anadarko E&P Offshore, LLC, 520 S.W.3d 39 (Tex. 2017).

355 *Id.* at 43.

356 *Id.*

357 *Id.*

358 *Id.*

359 *Id.*

360 *Id.* at 53.

361 *Id.* at 48-49.

362 *Id.* at 49.

363 *Compare Lightning Oil Co.*, 520 S.W.3d at 48-9 (seeking to square its analysis with the near absolute nature of the rights of the mineral estate as dominant estate), *with Crosstex*, 505 S.W.3d at 595 (requiring non-trifling interference with use for nuisance).

364 *Lightning Oil*, 520 S.W.3d at 53.

courts to intervene, one must prove a substantial impairment of one's use as opposed to a theoretical one.[365]

This logic extends further. Thus, one of the key remedies for a nuisance is abatement of the nuisance (its removal) and may involve self-help to bring it about.[366] This concept was further expanded in a commons-oriented fashion. In *Spur Industries, Inc. v. Del E. Webb Development Co.* the Supreme Court of Arizona was called upon to resolve the classic coming-to-the-nuisance case.[367] A real estate developer began developing a sub-division next to a feedlot.[368] The feedlot (predictably) emitted smells not to the liking of potential buyers in the subdivision.[369] The developer asserted a nuisance claim, relying particularly on the fact that the feedlot operator did not comply with health and safety ordinances by permitting conditions on its property that "constitutes a breeding place for flies, rodents, mosquitoes and other insects."[370] The feedlot owner defended on the basis that the developer had come to the nuisance.[371]

The case is interesting for its ultimate resolution of the dispute. The feedlot had to move.[372] This can easily be reconciled with the tort and fault-based conception of nuisance in the Restatement.[373] What cannot be reconciled with such a perspective is that the court also ordered the developer to pay for the move.[374] The ostensible victim of the nuisance had to pay for the removal of the nuisance.[375] This is not consistent with a fault-based understanding as the wrongdoer is not typically compensated to desist from their

---

365 For a full treatment of the question of subsurface rights in U.S. common law through the nuisance lens, see Joseph A. Schremmer, *Getting Past Possession: Subsurface Property Disputes as Nuisance*, 95 WASH. L. REV. 315, passim (2020). For its discussion of Lightning Oil Co., see *id.* at 361-64.

366 *Crosstex*, 505 S.W.3d at 610.

367 Spur Industries, Inc. v. Del E. Webb Development Co., 494 P.2d 700 (Ariz. 1972).

368 *Id.* at 705.

369 *Id.*

370 *Id.* at 706 (quoting ARIZ. REV. STAT. ANN. §36-601).

371 *Id.* at 706-07.

372 *Id.* at 708.

373 RESTATEMENT (SECOND) OF TORTS § 821B(2)(a) (AM. L. INST. 1979).

374 *Spur Industries*, 494 P.2d at 708.

375 *Id.*

wrongdoing.[376] Nuisance cannot be fault based if it can require contribution from the person seeking to enjoy their right to be put in a position to enjoy it.

But such a result is perfectly consistent with a commons rationale of nuisance as protecting the correlative rights of users of a commons. Maintenance of the commons requires contributions from all participants in the commons.[377] To demand one's right of access therefore also means that one must be willing to contribute to the maintenance of the commons. When such maintenance requires others to incur expenses, all must reasonably participate in them. Claiming a right to the commons is neither self-centered nor is it free. It is communal, and it is earned.

ii. France

As a quintessential civil law jurisdiction, France approaches the question of nuisance in a manner that is both startlingly different from and startlingly similar to U.S. law. The civil law tradition derives from and is a "reception of" the Roman law.[378] One of the most authoritative restatements of Classical Roman law is the *Digest of Justinian*.[379] The *Digest of Justinian* provides in relevant part that "every person may act as he pleases on his own property, so long as he immits [sic] nothing on the property of another."[380] This proviso provides the foothold for a conception of correlative rights in Roman law.

This Roman law principle was received in French law in terms of the "*droits de voisinage*," "*troubles de voisinange*," or "neighbors' rights. France exported its conception of *trouble de voisinage* in one

---

[376] The Court sought to avoid this conclusion by stating that the victims were the customers of the plaintiff and not the plaintiff and moving on an ostensible basis of comparative fault. *Id.* This rationale is difficult to maintain given that the Court ruled that the plaintiff had standing and the victims on whose behalf the Court appeared to act did not appear in the proceedings. *Id.* at 706.

[377] *See, e.g.*, OSTROM, *supra* note 2, at 82-7 (discussing early irrigation communities in the Philippines).

[378] Leon E. Trakman, *"Legal Traditions" and International Commercial Arbitration*, 17 AM. REV. INT'L ARB. 1, 5 (2006).

[379] *Id.*

[380] Zigurds L. Zile, *Judicial Control of Land Use in France*, 45 CORNELL L. REV. 288, 289 (1960) (translating Digest 8.5.8, § 5).

form or another to other jurisdictions. For example, the concept was incorporated in Senegalese civil law.[381]

These neighbors' rights on their face differ markedly from nuisance.[382] Nuisance distinguishes between public and private nuisance. Neighbors' rights deem that public nuisance is a question for administrative regulation as opposed to civil law rights.[383] Claims of public nuisance would have to be brought to "the authorities" as opposed to the courts.[384] All one could claim for, on its face, would be private nuisance and the private harm suffered by a neighbor as opposed to the harm done to the community.[385]

At the same time, neighbors' rights are startlingly similar to the law of nuisance. For one, neighbor's rights sit at the uneasy intersection of property law and the law of obligations, particularly delict (or tort).[386] Problematically, French civil law was historically incomplete and did not deal with the emission of gases, odors, noise, or vibrations from one property to the property of the neighbor.[387] This area of law therefore was developed by combining concepts from the right to exclude and the right of enjoyment in the law of property with the general delictual or tort principles that intentional or negligent conduct causing harm to another requires the payment of compensation.[388] This combination of areas of law permits French judges to enjoin fruitful and lawful use of land that is nevertheless unduly disruptive to the user's neighbors.[389]

French law is functionally similar to U.S. nuisance law and the law of correlative rights. It requires a showing of the invasion of

---

[381] *See* André Tunc, *La responsabilité civile dans trois récentes codifications africaines*, 19 REVUE INTERNATIONALE DE DROIT COMPARE 927, 931 (1967); *see also* DIDIER MARTIN, DROIT CIVIL ET COMMERCIAL SENEGALAIS 103-04 (1982) ; Ibrahima Ly & Papa Meissa Dieng, *Le Senegal*, *in* LA MISE EN OEUVRE NATIONALE DU DROIT INTERNATIONAL DE L'ENVIRONNEMENT DANS LES PAYS FRANCOPHONES 389, 399 (Michel Prieur ed., 2003).

[382] *See* Vanessa Casado Perez & Carlos Gomez Liguerre, *From Nuisance to Environmental Protection in Continental Europe*, 92 S. CAL. L. REV. 1003, 1010-11 (2019) (for a comparative analysis).

[383] Zile, *supra* note 380, at 294.

[384] Zile, *supra* note 380, at 294.

[385] Zile, *supra* note 380, at 294.

[386] Zile, *supra* note 380, at 294.

[387] Zile, *supra* note 380, at 294.; Casado, *supra* note 382, at 1010-11.

[388] Zile, *supra* note 380, at 297-8.

[389] ANNIE CHAMOULAUD-TRAPIERS, DROIT DES BIENS 167 (2d ed. 2007).

another's property right.[390] It further conceived of this invasion as coming from the use of a property right.[391] In short, it was an action that was as much in *rem*—about the land or lands involved—as it was in *personam*—about the owner of the land. This echoes American nuisance.[392] Similarly, it requires a showing of abuse of right.[393] This also mirrors American nuisance.[394] Finally, both require a showing of causation.[395]

The French understanding of abuse of right is particularly helpful to show the striking functional similarities between American nuisance and French neighbor's rights. An abuse of rights is the exercise of a right in a manner that is ultimately unreasonably destructive of the interests of another.[396] "Unreasonably destructive" here can be understood as disproportionately disruptive. This disproportion is then measured against neighborhood standards to determine whether the use of the land in question is normal or abusive.[397]

But it can also be understood as disruptive of the right of a neighbor to access to a commons or quasi commons. Specifically, the French law of neighborhood rights is historically concerned with rights to groundwater. In the neighborhood right context, early cases such as *Badoit v. André* or *Forissier v. Chaverot* stood for the proposition that groundwater rights are treated as a resource that cannot be unreasonably captured by any one person due to an absolute ownership claim—water does not belong to any one person.[398] Rather, in these historical cases, water may only be reasonably exploited or enjoyed by all who share in the reservoir.[399] French law here grappled with the same problem as the correlative rights and commons problem in U.S. law.

---

390 Zile, *supra* note 380, at 297-98; CHAMOULAUD-TRAPIERS, *supra* note 389, at 166-73.

391 Zile, *supra* note 380, at 297-98; CHAMOULAUD-TRAPIERS, *supra* note 389, at 166-73.

392 *Spur Industries*, 494 P.2d at 708.

393 Zile, *supra* note 380, at 297-98, 302-09; Casado, *supra* note 382, at 1010-11.

394 Wyche, *supra* note 333, at 357.

395 *Restat. 2d, supra* note 312, at § 822.

396 Zile, *supra* note 380, at 299-302.

397 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167-69.

398 *Badoit v. André*, Lyon, 18 avril 1856, D.P. [1856] 2. 199; *Forissier v. Chaverot*, Req., 10 juin 1902, D.P. [1902] 1. 454; *see also* Zile, *supra* note 380, at 299 (discussing both cases).

399 *See* Zile, *supra* note 380, at 299.

Similarly, in a modern setting, French neighbors' rights concern such resources as access to sunlight, quiet enjoyment, freedom from noxious smells, and a clean environment.[400] These resources, too, are characteristic of a commons. We all need them to thrive. We all share in them. And yet, no one person owns them as such. Nor has even the most totalitarian of governments nationalized or collectivized the air we breathe.

This understanding of the French law of neighbor's rights as maintaining the commons can explain a startling problem in French law. A judge establishes a violation of neighborhood rights based on the "abnormal character of the interference."[401] But, as a French property law hornbook makes clear, "a decision which would require proof of fault by the author of the interference would be commit an error of law."[402] How then could conduct be both abusive and not blameworthy at the same time?

The correlative-rights rationale provides an answer. The "over-enjoyment" of a commons, taken to an extreme, threatens the commons itself. Such over-enjoyment sets the stage for the famous tragedy of the commons of collective unsustainable use.[403] It is abnormal and abusive in the sense that it is unsustainable.[404]

And yet, it is precisely what makes the tragedy of the commons tragic that blaming the participants for their individual overuse of the commons is as misguided as it is pointless.[405] This individual overuse is an understandable and rational response to structural incentives to take while something is still available to be taken.[406] This response is understandable and not blameworthy because the abstention of each individual user of the commons alone would only inflict a double loss on that individual—loss of use of the commons now relative to other users of the commons and a loss of the commons later when the unsustainable use by others has finally driven the commons to extinction.[407] The tragedy is structural and not individual.[408]

---

400 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167-69.

401 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167.

402 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167.

403 Hardin, *supra* note 222.

404 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167-69.

405 *See* OSTROM, *supra* note 32, at 178-80.

406 OSTROM, *supra* note 32, at 178-80.

407 OSTROM, *supra* note 32, at 178-80.

408 OSTROM, *supra* note 32, at 178-80.

The hornbook distinction between fault and abnormal use in the French law of neighbor's rights captures the essence of this tragedy and seeks to set the structural incentives to avert it.[409] It understands that the conduct by the person is not blameworthy. It nevertheless maintains that the use of the resource is abusive and abnormal and as such to be enjoined to protect the commons.[410] The commons rationale thus brings the law back to understanding of a principle of nuisance as between property and tort/delict, between *in personam* and *in rem* by focusing on the structural consequences of correlative use of resources.[411] The French commons rationale, however, is more protective than some U.S. jurisdictions, such as Texas, by allowing a cause of action for conduct, which is abnormal in its surroundings even if it is not ultra-hazardous.[412]

Given this functional understanding of French neighbor's rights, it should not come as a surprise that French law resembles the American concept of nuisance law in another, central respect. Its main remedy, too, is abatement.[413] This means that like American nuisance tort law, it is currently a chief means to provide private law remedies for pollution.[414] It is thus inherently linked to environmental protection in its modern incarnation in the same way as nuisance law in America has become.[415] Both are means to help govern the commons.

iii. Russia

Russian law, as a civil law jurisdiction, follows broadly in the same legal tradition as French law. It is therefore unsurprising that Russian law follows broadly a similar starting point to French law in the use of property: as a matter of "private law, the interests of

---

409 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167.

410 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167.

411 This understanding of neighbor's rights in French law is currently in the process of codification. *See* Casado, *supra* note 382, at 1011, for an English translation of the draft text and status of the codification process.

412 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167; *Crosstex*, 505 S.W.3d at 607-08.

413 11 INTERNATIONAL ENCYLOPEDIA OF COMPARATIVE LAW, TORTS 56 (Andre Tunc ed. 1981)

414 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167.

415 *See* Monika Hinteregger, *Environmental Liability*, *in* THE OXFORD HANDBOOK OF COMPARATIVE ENVIRONMENTAL LAW (Emma Less & Jorge E. Viñuales, eds., 2019).

other persons, in particular, neighbors must be taken into account."[416] The key property law provision in the Code dealing with a question akin to nuisance is Article 304. It states that "[a]n owner may demand the elimination of all violation of its rights even though these violations were not connected with a deprivation of possession."[417] There is thus a foothold for correlative rights to develop in Russian Law, as well.

Article 304 of the Russian Civil Code codifies the Roman law "*actio negatoria*."[418] This "*actio negatoria*" is originally a Roman law cause of action available to an owner of land to force another to cease and desist from interfering with the owner's enjoyment of his or her land.[419] Roman law construed such interference with enjoyment as a servitude imposed upon the land.[420] The *actio negatoria* sought a declaration of the absence of such a servitude and an injunction against the offending interference.[421] The failure to seek such a declaration could itself be problematic, as a servitude could be imposed upon land by prescription (adverse possession).[422] As one recent Roman law text explains, the *actio negatoria* therefore "served to defend against claims of servitudes, 'immissions [sic]' [*i.e.*, the commissions of what at common law would be called nuisance or trespass], and other impairments of ownership."[423] This concept of *actio negatoria* is a typical civil law meaning to protect use rights and

---

416 PETER B. MAGGS, OLGA SCHWARTZ & WILLIAM BURNHAM, LAW AND LEGAL SYSTEM OF THE RUSSIAN FEDERATION 417, 436 (2015).

417 GRAZHDANSKIĬ KODEKS ROSSIĬSKOĬ FEDERATSII [GK FK] [Civil Code] arts. 304 (Russ.) (translated in PETER B. MAGGS, THE CIVIL CODE OF RUSSIA, PARTS 1 AND 2 (2018)).

418 Tikhon Podshivalov, *Models of* Actio Negatoria *in the Law of Russia and European Countries*, 7 RU. L.J. 128, 133 (2019)

419 *See* W.W. BUCKLAND REVISED BY PETER STEIN, A TEXT-BOOK OF ROMAN LAW FROM AUGUSTUS TO JUSTINIAN 676 (3d ed. 2007) (discussing the "need for this action").

420 EUGENE PETIT, TRAITE ELEMENTAIRE DU DROIT ROMAIN para. 773 (1906).

421 *Id.*

422 *See* Max Radin, *Fundamental Concepts of Roman Law*, 13 CAL. L. REV. 207, 217 (1925) (discussing permissibility of acquisitive prescription of servitudes in praetorian law); *see also* A. N. Yiannopoulos, *Creation of Servitudes by Prescription and Destination of the Owner*, 43 LA. L. REV. (1982) (discussing creation of servitudes by prescription in modern civil law).

423 HERBERT HAUSMANIGER & RICHARD GAMAUF, A CASEBOOK ON ROMAN PROPERTY LAW 205 (George A. Sheets trans. 2012).

is prevalent in other jurisdictions in Latin America such as Brazil, as well as many Eastern European jurisdictions.[424]

Article 304 of the Russian Civil Code has been interpreted in express comparison to the common law of nuisance.[425] This comparison is functionally apt—nuisance and *actio negatoria* regulate the same kind of correlative relationship. It is, however, formally somewhat problematic because Article 304 of the Russian Civil Code is structurally more closely related to property law than it is to delictual liability.[426]

This formal difference is blunted somewhat in practice. Conduct that satisfies this requirement of Article 304 further arguably meets the requirement of quasi-delictual liability in Russian law. Specifically, Russian law makes available injunctions for potential or future interferences with the enjoyment of property as part of its law of delict or tort.[427] This tort, too, has been analogized to the common law of nuisance.[428] These requirements meaningfully overlap with, and inform the property law concept codified in Article 304 of the Civil Code.[429]

To succeed on a claim for violation of Article 304, jurisprudence sets out that the claimant must prove ownership of property.[430] This tracks the French understanding of neighbors' rights. Both Russian law and French law formally require that the interference suffered be a private wrong only.[431] That is, in both Russian law and French

---

424 *See* Jose Isaac Pilati, *Property Law*, *in* INTRODUCTION TO BRAZILIAN LAW at § 5.01 (Fabilan Deffenti & Weiber Barral eds., 2016); *see also* Podshivalov, *supra* note 418, *passim*.

425 *See* Podshivalov, *supra* note 418, at 131 (comparing actio negatoria to English law); *see also* Stanley R. Boots, *Observations from Afield: The Tension Between the Goals of Russian Environmental Legislation and Extralegal Factors in the Russian Far East*, 10 INT'L LEGAL PERSP. 201, 234 (1998) (comparing the Russia legal system to U.S. environmental law).

426 *See* GRAZHDANSKIĬ KODEKS ROSSIĬSKOĬ FEDERATSII [GK RF] [Civil Code] arts. 301-304 (Russ.) (providing the immediate context for article 304).

427 CHRISTOPHER OSAKWE, RUSSIAN CIVIL CODE TEXT AND ANALYSIS, pts. 1-3, at 215-16 (2008).

428 *Id.*

429 GRAZHDANSKIĬ KODEKS ROSSIĬSKOĬ FEDERATSII [GK RF] [Civil Code] art. 304 (Russ.) (translated in PETER B. MAGGS, THE CIVIL CODE OF RUSSIA, pts. 1-2 (2018)).

430 Podshivalov, *supra* note 418, at 142 (discussing Novosibirsk Regional Court Determination of 16 May 2017 in case No. 33-4705/2017).

431 *See* Asya Ostroukh, *Russian Society and its Civil Codes: A Long Way to Civilian Civil Law*, 6 J. CIV. L. STUD. 373, 393 (2013):

law, the plaintiff must have standing to bring a lawsuit and allege a specific harm to a specific piece of property and a specific property right. Both appear to exclude a public wrong or public nuisance.[432]

Further, the plaintiff must prove that he or she "does not have different means to freely use the object belonging to him [or her]."[433] The cause of action applies not just to physical intrusions, but also to deprivations of light and similar environmental harms.[434]

In addition to these requirements, an action for violation of Article 304 also takes on elements of delictual liability much like U.S. nuisance and French neighborhood rights. Specifically, the conduct at issue in an Article 304 violation must be "wrongful." As a recent study explains, the conduct is wrongful if it "is carried out arbitrarily, without authorization, without a sufficient legal basis."[435]

Importantly, the understanding of wrongfulness here tracks the French understanding of abnormal use.[436] Thus, in Russian law, wrongfulness does not mean fault or guilt.[437] This, too, was a hallmark of the French neighbors' rights and its link to the protection of the enjoyment of the commons.[438]

The quintessential protection of enjoyment at issue in Russian sources again indicates a close link to correlative rights. The

---

> Nonetheless, in spite of all these restrictions, it is a private property that gives to its owner all the rights of possession, enjoinment, and disposition of property. This right is also protected by all of the means of private ownership known to civilian legal systems (a true revendicatory action/actio rei vindicatio and negatory action/actio negatoria). Vladimir Gsovski is correct in his statement that, "the Soviet law of property shows also how inescapable private ownership, although in a small dose, is, even in a socialist State."

(internal italics omitted) (quoting VLADIMIR GSOVSKI, 2 SOVIET CIVIL LAW: PRIVATE RIGHTS AND THEIR BACKGROUND UNDER SOVIET REGIME 567 (Univ. of Mich. L. Sch. Ann Arbor 1949); CHAMOULAUD-TRAPIERS, *supra* note 389, at 167-69.

[432] Podshivalov, *supra* note 418, at 142 ("[W]hen making a statement of actio negatoria, the claimant must prove that he has the appropriate right to an individually-defined object."); CHAMOULAUD-TRAPIERS, *supra* note 389, at 167-69.

[433] Podshivalov, *supra* note 418, at 143.

[434] Podshivalov, *supra* note 418, at 152.

[435] Podshivalov, *supra* note 418, at 150.

[436] *Compare* CHAMOULAUD-TRAPIERS, *supra* note 389389, at 167 (outlining French understanding of abnormal use), *with* Podshivalov, *supra* note 418, at 143 (outlining the Russian understanding).

[437] Podshivalov, *supra* note 418, at 143 ("Actio negatoria will be satisfied only if the wrongfulness of the actions of a third party is proved, and it does not matter if this behavior was guilty.").

[438] *See infra* Section II.

interference at issue in the Russian law conception of *actio negatoria* inherently is an interference with *use* of property. It is not an action to quiet title—in fact, it is defined in contradistinction to such an action.[439] Rather, it is an action to enjoin interference with enjoyment.

The protection of use is a protection of a property right because "interfering with the ability to extract useful properties from an object by one's actions automatically entails difficulty in owning it."[440] The protection of *actio negatoria* therefore applies to the over-extraction by another of resources shared in the sense of correlative rights in the same way as the abuse of right rationale did in the French water law context.[441] The *actio negatoria* seeks to protect the reasonable use of owners with interests in a shared resource.

Two recent case examples showcase this understanding of Russian law. The first, Case No. 18AP-10608/2016, concerns the release of wastewater by a wastewater treatment facility.[442] The facility impaired the use of its property by a neighboring property owner due to contamination in violation of Russian water law.[443] The conduct was enjoined, the nuisance abated—and it was enjoined to protect the use of the plaintiff's correlative right to the shared water supplies. [444] The defendant's water use threatened the shared water rights and therefore was to be enjoined.[445] Second, the Russian Supreme Court in 2012 applied a similar understanding to a more mundane and urban setting:[446] the interference with the enjoyment of common areas in an apartment building.[447] The protection therefore applies to access to commons or shared resources broadly defined.

In sum, Russian law is broadly consistent with American and French law. It concerns the protection of correlative rights in

---

[439] Podshivalov, *supra* note 418, at 144-45 (listing the legal characteristics of actio negatoria).

[440] Podshivalov, *supra* note 418, at 147.

[441] Podshivalov, *supra* note 418, at 147 (discussing Russian law); *see also Badoit v. André Lyon*, 18 avril 1856, D.P. [1856] 2. 199 (Fr.); *Forissier v. Chaverot*, Req., 10 juin 1902, D.P. [1902] 1. 454 (Fr.); Zile, *supra* note 380, at 299 (discussing both French cases).

[442] Podshivalov, *supra* note 418, at 155.

[443] Podshivalov, *supra* note 418, at 155.

[444] Podshivalov, *supra* note 418, at 155.

[445] Podshivalov, *supra* note 418, at 155.

[446] Podshivalov, *supra* note 418, at 153 (discussing the Supreme Court of the Russian Federation of 17 February 2015 in case No. 302-ES14-1496).

[447] Podshivalov, *supra* note 418, at 153.

commons. Russian law polices the use of the common pooled resource against interferences with correlative rights. It polices the use not by reference to the concept of fault. Rather, it looks to a concept of wrongfulness that, like the French concept of abnormal use, is concerned with the sustainable use of resources.

iv. People's Republic of China

Chinese law similarly recognizes a private right of action for nuisance. In principle, non-trivial interferences with a property right can give right to a suit in nuisance.[448] This principle has since been expanded and further defined in a concept of statutory nuisance. As Professor Guiguo Wang explains, first attempts at codifying statutory nuisance was intended as a "bridge between the common law and regulations."[449] Professor Wang notes that "[s]tatutory nuisance was created to allow for a speedy and efficient way to abate nuisances without resorting to [the] complex" regulatory procedures.[450] Chinese law has since undergone further reform.

The currently most analogous provisions in Chinese law to nuisance are Articles 65-68 of the 2010 Chinese Tort Law.[451] Article 65 follows the general polluter-pays principle.[452] It sets out that if a person suffering from pollution can show that they were harmed and that the harm was caused by the pollution, the person who caused the pollution will be liable to the victim.[453]

Once a party has discharged its burden under Article 65, Article 66 imposes the burdens of persuasion onto the polluter to show that their activity did not constitute pollution.[454] Further, Article 66 allows the polluter to claim for mitigation or to provide evidence to

---

448 THE CHINA LAW SERIES, LEGAL DEVELOPMENTS IN CHINA: MARKET ECONOMY AND LAW 414 (GUIGUO WANG & Wei Zhenying eds., 1996).

449 *Id.* at 420.

450 *Id.*

451 Zhōnghuá rénmín gònghéguó qīnquán zérèn fǎ (中华人民共和国侵权责任法) [Tort Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010) arts. 65-68 (China), https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn136en.pdf [https://perma.cc/WZL6-6XT7] (WIPO, trans.).

452 *Id.* at art. 65.

453 *Id.* at art. 66.

454 *Id.*

call into question the plaintiff's causation case.[455] The remaining two articles of Chapter VII on environmental pollution further set out a modified regime of joint and several liability.[456]

This new 2010 regime has been likened to private nuisance.[457] It tracks some of the features of French and Russian law and a majority of U.S. jurisdictions. Specifically, the 2010 Tort Law creates a no-fault regime.[458] This no-fault regime, however, does not outright define what constitutes "pollution."[459] It thus does not identify clearly whether the pollution in question means any emissions or interferences or only abnormal emissions or spills. It also does not list what kind of interferences will be considered pollution.

The question as to what pollution is covered by the 2010 regime can meaningfully be informed by the broader public interest environmental lawsuits now available under Chinese law.[460] This broader Chinese law framework permits lawsuits not just by persons directly harmed by pollution, as the 2010 Tort Law would.[461] It removes this standing requirement and allows public interest groups to bring actions for environmental harm in the courts.[462]

The definition of pollution operating under this broader framework, as Professor Benoit Mayer and Richard Zhang explain, allows public interest litigation "to target not only conduct which pollutes the human environment, but also actions that cause ecological damage."[463] A systemic interpretation of Chinese law as a whole would suggest that the term "pollution" in the 2010 Tort Law follows this broader concern with pollution and would allow suit for any unreasonable environmental degradation.[464]

This link again recalls the relationship between nuisance and commons governance. The use of common pooled resources by one party unreasonably impairs the use of the same resource by others.

---

455 *Id.*

456 *Id.* at arts. 67-68.

457 Carissa Wong, *Director Duty of Care in China and the United States: What Liability for Climate Change?*, 18 VT. J. ENV'T. L. 287, 301-02 (2016).

458 *Id.* at 302-03.

459 Tort Law of the People's Republic of China, *supra* note 451.

460 *See* Richard Zhang & Benoit Mayer, *Public Interest Environmental Litigation in China*, 1 CHI. J. ENVTL. L. 202 (2017) (discussing public interest environmental litigation in China).

461 Tort Law of the People's Republic of China, *supra* note 451 at ch.II.

462 Zhang & Mayer, *supra* note 460, at 203.

463 Zhang & Mayer, *supra* note 460, at 217.

464 Zhang & Mayer, *supra* note 460, at 217-18.

Both the 2010 Tort Law and the broader statutory framework of which it forms part appear aimed at righting this commons problem and provide a remedy and a means to gain access to justice for those negatively affected by over-exploitation.[465]

The link between tort law and commons is the more pronounced in the Chinese setting. The public interest portion of Chinese environmental protection litigation is rooted in a conception of an "ecological civilization."[466] This ecological civilization protects the commons by providing a "sound working and living environment."[467] This is a classical commons concern at the core of the American, French, and Russian conceptions of nuisance.

Moreover, the Chinese conception also covers cultural commons.[468] The environmental law framework is available in order to protect cultural relics against deterioration.[469] This again creates a strong link between heritage, commons protection, and Chinese tort law in this broader setting.

There are, however, notable differences between Chinese law and the other legal systems studied so far. Most significantly, the other legal systems studied so far have located nuisance principles at the intersection between property and tort law.[470] They have focused on the flipsides of use and interference through use through this lens of positive property rights to utilize one's property and negative property rights to exclude others from interfering in one's own property rights.[471]

Chinese law does not locate the concern with commons protection at this intersection of property and tort law. Rather, Chinese law places this concern at the intersection of tort and administrative law.[472] This suggests a completely different theoretical approach to the problem of commons governance than nuisance law would suggest.

---

465 Zhang & Mayer, *supra* note 460, at 217-18.

466 Zhang & Mayer, *supra* note 460, at 209; Sun Qian & Jack Tuholske, *An Exploration of and Reflection on China's System of Environmental Public Interest Litigation*, 47 ENVTL. L. REP. 10497, 10501-02 (2017).

467 Zhang & Mayer, *supra* note 460, at 209; *see also* Sun & Tuholske, *supra* note 466.

468 Zhang & Mayer, *supra* note 460, at 218.

469 Zhang & Mayer, *supra* note 460, at 218.

470 *See infra* Sections I-III.

471 *See infra* Sections I-III.

472 *See* Zhang & Mayer, *supra* note 460.

This difference does not, however, undercut the core commonalities of a nuisance principle established so far. Thus, the regime still places a premium on policing the use of shared resources (the environmental and cultural heritage).[473] It does not approach the question of permissibility or impermissibility through the lens of fault.[474] Even more starkly than the other approaches investigated so far, Chinese law looks to sustainability as the main goal post of commons governance.[475]

Perhaps most surprisingly, Chinese law in this broader legal infrastructure places governance of the commons in the hands of multiple actors. It does not rely upon a regulatory approach. Rather, it relies upon a combination of private and governmental mechanisms to govern the commons.[476] This combination consists of private rights to participation in the commons with public enforcement mechanisms for the protection of these rights.[477] These public enforcement mechanisms, however, remain split between state-driven supervision through the administrative process and private enforcement through tort and public interest litigation.

v. Israel

Israel is a mixed jurisdiction, inhabiting a place between the civil and (English) common law. The main instrument governing tort law in Israel, the Civil Wrongs Ordinance of 1944, is English in origin.[478] The Civil Wrongs Ordinance "constitutes a sort of Restatement of the common law of torts, as it stood during the 1930's and 1940's."[479] This Ordinance, as updated, continues to provide the foundation for tort law in Israel.[480]

---

473 Zhang & Mayer, *supra* note 460, at 217-18; Sun & Tuholske, *supra* note 466.

474 Wong, *supra* note 457.

475 Zhang & Mayer, *supra* note 460, at 217-18; Sun & Tuholske, *supra* note 466.

476 Zhang & Mayer, *supra* note 460, at 217-19.

477 Zhang & Mayer, *supra* note 460, at 217-19.

478 Aharon Barak, *The Codification of the Civil Law and the Law of Torts*, 24 ISR. L. REV. 628, 639 (1990).

479 *Id.*

480 Civil Wrongs Ordinance, 5712-1968, LSI 10 266 (Isr.), https://www.israelinsurancelaw.com/tort-ordinance-new-version-updated-to-march-2015/ [https://perma.cc/WXX6-XVCZ]. In addition to the tort of nuisance, Israeli law also has a criminal nuisance statute. This section deals with the private

The Civil Wrongs Ordinance contains a section on nuisance. Given its common law origin, it unsurprisingly distinguishes between public nuisance and private nuisance. It codifies the law of public nuisance in sections 42 and 43.[481] It codifies the law of private nuisance in sections 44 to 46.[482] It defines a public nuisance as "some unlawful act, or omission to discharge a legal duty, where such act or omission endangers the life, safety, health, property or comfort of the public or obstructs the public in the exercise of some common right."[483] It requires an individual to have standing to bring an action of public nuisance.[484]

The Civil Wrongs Ordinance defines private nuisance as conduct or use of immovable property so "as materially to interfere with the reasonable use and enjoyment, having regard to the situation and nature thereof, of the immovable property of any other person."[485] The Civil Wrongs Ordinance further codifies defenses, establishing that consent is a defense to nuisance whereas moving to the nuisance is not.[486]

Like the other legal systems studied, Israeli law used private nuisance as a means to provide private redress for pollution. One of the earliest cases using the nuisance section of the British-mandate Ordinance was *Sick Fund of the General Federation of Jewish Labour in Palestine v. Taasiya Chemith*.[487] The case concerned the emission of gases from a chemical plant.[488] These emissions ended up in a hospital, causing dizziness and headaches in its patients.[489] The Tel Aviv District Court found that the emission constituted a nuisance.[490]

---

law statute. For a discussion on the relationship between the two, see Rachelle Adam, *Government Failure and Public Indifference: A Portrait of Water Pollution in Israel*, 11 COLO. J. INT'L ENVTL. L. & POL'Y 257, 311-12 (2000).

481 Tort Ordinance, 5712-1968, §§ 42-43 LSI 10 266 (Mar. 2015) (as amended) (Isr.), https://www.israelinsurancelaw.com/tort-ordinance-new-version-updated-to-march-2015/ [https://perma.cc/WXX6-XVCZ].

482 *Id.* at §§ 44-46.

483 *Id.* at § 42.

484 *Id.* at § 43.

485 *Id.* at § 44(a).

486 *Id.* at §§ 45-46.

487 Zeev Negbi, *The Prevention of Nuisances in Israel*, 11 INT'L & COMP. L.Q. 822, 826 (1962).

488 *Id.*

489 *Id.*

490 *Id.*

The perhaps paradigmatic cases for such a use of private nuisance in Israeli jurisprudence is *Ata Textile Co. Ltd. v. Schwartz*.[491] The case involved an aggrieved homeowner, Mr. Schwartz.[492] Mr. Schwartz lived on the edge of a residentially zoned area abutting an industrial area.[493] Mr. Schwartz had the misfortune to have Israel's largest textile factory belonging to Ata Textile Co. Ltd. for a neighbor.[494] Ata had installed cooling equipment essential to its production methods in its factory.[495] Unfortunately, first for Mr. Schwartz and then for Ata, the equipment "caused tremendous noise in Mr. Schwartz's home."[496] Mr. Schwartz took Ata to court and sought an injunction to make it stop.[497]

The case is paradigmatic for nuisance law because it allowed for the issuance of an injunction enjoining the nuisance even though the hardship of the injunction to the defendant was greater than the harm of the original nuisance to the plaintiff. In other words, nuisance law is not only a means to receive compensation.[498] It creates a positive duty to cease and desist from creating a nuisance.

The case is interesting in another regard. There is no sense in which Ata's conduct could have been culpable or even negligent. Ata did not install the equipment in order to harm Mr. Schwartz.[499] Ata installed cooling equipment that was appropriate for its own purposes and apparently did so in a manner consistent with industry standards, or at the very least in a manner that would have satisfied an economic analysis of relative benefits and harms.[500] Mr. Schwartz's expectation of quiet was a reasonable use and enjoyment of his house,[501] and the level of noise generated by Ata's cooling

---

491 CivA 44/76 Ata Textile Company Ltd. v. Schwartz, 30(iii) P.D. 785 (1976) (Isr.). *See* Barak, *supra* note 478, at 642 n90 (discussing the paradigmatic nature of the case); Perry, *infra* note 498; Adv. A. Amos Fried, *A brief review of the law of nuisance*, JANGLO (November 11, 2018) https://www.janglo.net/item/9nVdowOCukq [https://perma.cc/ZRM5-AJSG].

492 David Kretzmer, *Judicial Conservativism v. Economic Liberalism: Anatomy of a Nuisance Case*, 3 ISR. L. REV. 298, 304 (1978).

493 *Id.*

494 *Id.*

495 *Id.*

496 *Id.* at 304-05.

497 *Id.* at 305.

498 Ronen Perry, *Law of Torts*, *in* THE ISRAELI LEGAL SYSTEM 87, 109 (Christian Walter et al. eds., 2019).

499 Kretzmer, *supra* note 492, at 304-06.

500 Kretzmer, *supra* note 492, at 304-06; Perry, *supra* note 498, at 88-89.

501 Perry, *supra* note 498, at 88-89.

equipment substantially interfered with it.[502] The case therefore illustrates that the understanding in Israeli law of a substantial interference with reasonable use and enjoyment is consistent with the civil law understanding of neighbor's rights or the *actio negatoria*: it operates without fault but with regard to the reasonableness of use seen from the perspective of the commons.[503]

Both features of nuisance law are consistent with the function of nuisance laws outlined above to protect the commons against over-use and interference with correlative rights. In *Schwartz*, this common resource was the quiet enjoyment of a residential environment, pun intended.[504] Any student who was unexpectedly exposed to noise while studying for a law school exam can personally confirm that quiet is a resource. The problem is, as the same student may also painfully recall, it is a common pooled resource. A room is only quiet when all are silent. It was to protect this common pooled resource of "quiet" that the court issued an injunction—even though the injunction was not economically advantageous. That is to say, the Court protected the commons from tragedy by allowing Mr. Schwartz to prevent the "over-use" of the noise threshold in the neighborhood through a nuisance action.[505]

One should not misunderstand the result in *Schwartz* as an absolute injunction against use of commons whenever such use interferes with interest of a neighbor. To the contrary, the Israeli Supreme Court in the earlier decision in *Azari v. Victor Klein* explained that the test is one of mutuality, reciprocity, and reasonableness.[506] In terms of the commons, each member of the relevant community of interests has correlative rights to reasonable access to the commons. Any insistence by one member of the community that would render the commons useless to the others would in Israeli terms be unreasonable and lacking in mutuality.[507] In French civil law terms, it would amount to an abuse of right.[508] In

---

502 Perry, *supra* note 498, at 88-89.

503 *See infra* Sections V(b)(ii)-(iii); *see also* Civil Wrongs Ordinance, *supra* note 481, at § 44(a). *See generally* Daphna Lewinsohn-Zamir, *Do the Right Thing: Indirect Remedies in Private Law*, 94 BOS. U. L. REV. 55, 93 n.199 (2014) (discussing that nuisance is between strict and fault-based liability).

504 *See* Kretzmer, *supra* note 492, at 304-05.

505 Perry, *supra* note 498, at 109-10.

506 *See* Negbi, *supra* note 487, at 828.

507 *See* Negbi, *supra* note 487, at 828.

508 *See infra* Section V(b)(ii).

short, the nuisance principle is one that applies to the use of commons in context and in the interaction between its users and thus takes into account the plurality of interests and uses involved.

This feature of nuisance therefore leaves a significant autonomy with the users of the commons. Mutuality and reciprocity are concepts that assume communication and an attempt at reasonable self-regulation of the commons.[509] The law of nuisance superimposes oversight over these self-regulatory processes to secure both the enforceability of reasonable reliance interests of participants and an appropriate incentive structure to avoid recourse to the courts as a means of last resort—a recourse that might end in an all-or-nothing injunction *ex post* rather than accommodation between the parties as to how use might be curtailed in a reasonable manner.

Despite some practical divergence of public nuisance law in Israel,[510] the key principle of nuisance in Israeli law largely tracks the principle of nuisance law and correlative rights as it has been developed on the basis of American, French, Russian, and Chinese law. Israeli law confirms the purpose of nuisance law to protect commons by focusing on the relative uses of the commons. Nuisance law protects the commons while leaving significant flexibility to the users of the commons to determine their own rules for access and use of the commons. It thus does not impose an absolute or hard rule of nuisance, but rather looks to a principle of nuisance to support the development of an equilibrium by and between commons users.

vi. Shari'a

Shari'a similarly richly incorporates the principle of protecting the commons. The relationship between humans and creation is one cornerstone for protecting the commons. *Shari'a* places humans in a position of stewardship.[511] This stewardship entails the obligation

---

[509] *See* Negbi, *supra* note 487, at 828; ELINOR OSTROM, THE FUTURE OF THE COMMONS 79-80 (2012) (discussing the importance of asking questions and building trust and growing social capital by doing so).

[510] *See* Orit Marom-Albeck & Alon Tal, *Upgrading Citizen Suits as a Tool for Environmental Enforcement in Israel: A Comparative Evaluation*, 34 ISR. L. REV. 373, 400-401 (2000).

[511] Ali Ahmad, *Islamic Water Law as an Antidote for Maintaining Water Quality*, 2 U. DENV. WATER L. REV. 169, 178-9 (1999).

to protect and care for the environment, in other words, creation.[512] In principle, this obligation is not focused exclusively on human flourishing.[513] It extends to the protection of nature as a whole in its own right.[514]

This obligation is put expressly in terms of the commons. As one scholar puts it, "misuse might result in unjustly depriving future generations of the ability to benefit from them, and thus would also contradict the teachings of the True Faith and the stewardship of Man on Earth."[515] This rationale tracks closely the rationale of the tragedy of the commons to enjoin overuse so as to prevent the collapse of the commons.[516]

Shari'a fully internalizes this rationale. In a metaphor that is meaningful for current purposes, "[i]n the Islamic perspective, people in a community can be compared to passengers on a ship."[517] This life imposes "a common responsibility"[518]—and thus creates correlative rights. This responsibility means that "[e]ach passenger has to ensure the ship's safeguard not only for his own safety but that of others as well."[519] To disrupt the environment consequently "contradicts the principle that one should not cause environmental harm (embodied in Islamic Law (*Shari'a*))."[520] This principle again is broader than maintaining natural resource for future, human exploitation: "[e]xcessive exploitation of the environment driven by insatiable consumerism, individual economic gain, or limitless development, is hardly consistent with the trusteeship of humankind over all other matters."[521]

This principle is further expressed in a manner reasonably close to the French concept of neighbor's rights discussed above.[522] The Quran requires that one do good to "the near neighbor[s], the

---

512 Omar A. Bakhashab, *Islamic Law and the Environment: Some Basic Principles*, 3 ARAB L.Q. 287, 287-8 (1998).

513 Ahmad, *supra* note 511, at 178.

514 Ahmad, *supra* note 511, at 178.

515 Bakhashab, *supra* note 512, at 289.

516 *See* Hardin, *supra* note 215, at 1244-45.

517 Bakhashab, *supra* note 512, at 289.

518 Bakhashab, *supra* note 512, at 289.

519 Bakhashab, *supra* note 512, at 289.

520 Bakhashab, *supra* note 512, at 290.

521 Ahmad, *supra* note 511, at 179.

522 *See infra* Section V(b)(ii).

neighbor farther away."[523] This duty forms part of *Shari'a*.[524] This principle is close in expression to the requirement to act with due regard for one's neighbor and neighborhood usage underlying French neighbor's rights.[525] If anything, *Shari'a* extends this obligation further than French law because it covers neighbors near and far.[526] Further, it requires more expressly that the conduct of one not destroy the rights of use of another even if such use were otherwise consistent with community practice.[527]

This principle of *Shari'a* found expression in a manner very close to contemporary understandings of nuisance in the *Medjellè*, the Ottoman civil code. The *Medjellè* "prohibited [the] serious hinderance [sic] of those living in neighboring buildings, *inter alia*, byexcessive [sic] smoke or odour from a furnace or manufactory of linseed."[528]

In the land use context, too, *Shari'a* remains largely consistent with the understanding of nuisance developed above. In this context, too, "a person may undertake any kind of activity on his land to the extent that he does not degrade it or expose any beings, human or non-human, to danger."[529] Land use is circumscribed by obligations to warn and obligations to pay damages for lawfully conducted ultra-hazardous activities.[530] But again, these activities must be conducted in the context of neighbor's rights as outlined, for example, in the *Medjellè*.[531]

This obligation grows more stringent the more essential the commons affected by human conduct. For example, the obligation

---

[523] Quran, Surah Ah-Nisa 4:36, QURAN.COM, https://quran.com/4/36?translations=27,22,21,20,95,19,18,17,101,34 [https://perma.cc/YP6D-UKF5] (last visited Mar. 4, 2021).

[524] Bakhashab, *supra* note 512, at 290.

[525] *Compare* Bakhashab, *supra* note 512, at 290 (requiring one to take regard for one's neighbors), *with* CHAMOULAUD-TRAPIERS, *supra* note 389, at 167 (requiring as a matter of French law that activities not be unduly impairing the enjoyment of one's neighbor's rights).

[526] Quran, *supra* note 523.

[527] Bakhashab, *supra* note 512, at 289.

[528] MARTINUS NIJHOFF PUBLISHERS, TRANSBOUNDARY AIR POLLUTION: INTERNATIONAL LEGAL ASPECTS OF THE CO-OPERATION OF STATES vii (Cees Flinterman et al. eds., 1986).

[529] Ahmad, *supra* note 511, at 180.

[530] Umar F. Moghul & Samir H.K. Safar-Aly, *Green Sukuk: The Introduction of Islam's Environmental Ethics to Contemporary Islamic Finance*, 27 GEO. INT'L ENV'T L. REV. 1, 15-16 (2014).

[531] *See* TRANSBOUNDARY AIR POLLUTION, *supra* note 514.

"is more pronounced in the case of water."[532] The justification for this heightened standard is expressly commons-based—water is different because it "is a resource held in common by society."[533] This common ownership, and community right to water use, was also codified in the Ottoman *Medjellè*.[534]

Interestingly, the *shari'a* approach, too, rejects absolutism. Centrally, Islamic "[j]urists endeavored to balance strong individual rights against collective community rights including non-human components of nature, and to remain within the parameters of the intent and objectives of The Lawgiver."[535] It thus embeds the concept of nuisance in the relationships between users of commons and the commons itself. This again demonstrates a contextual approach, taking into account the autonomy of different actors in shaping how environmental nuisance principles are actually applied and the manner in which correlative rights are protected.

c. Applying Nuisance to the Cyber Context

The nuisance principle developed in the previous section functions to protect the rights of all participants in a commons against substantial interference with their enjoyment of the commons. It does so by treating the participants in the commons as correlative rights holders. These correlative rights secure that all participants in a commons maintain the commons and that none substantially interfere with the reasonable enjoyment of the commons by others. As such, nuisance promises to be a principle that can guide legal decision making in the cyber context. This section outlines how cyber nuisance would improve upon the blind spots in *Tallinn 2.0* addressed above in key respects.

---

532 Ahmad, *supra* note 511, at 180.

533 Ahmad, *supra* note 511, at 180.

534 Moghul & Safar-Aly, *supra* note 530, at 16.

535 Moghul & Safar-Aly, *supra* note 530, at 14.

i. Debugging the Fault Trap

One of the key problems bedeviling *Tallinn 2.0* was its insistence upon fault.[536] *Tallinn 2.0* follows a responsibility paradigm.[537] Thus, logically, it must also follow a full-blown fault paradigm. This led to significant governance issues, particularly as a fault paradigm did not provide for any realistic means to improve governance.

Cyber-nuisance changes the equation. It treats cyber as a commons. It therefore treats all participants in cyber as holding correlative rights to cyberspace.[538] These correlative rights require the maintenance of the resource as to which multiple parties hold correlative rights, which in the case of the current inquiry is cyberspace.[539] At times, this means one will need to help defray the costs of additional efforts by others to maintain the commons.[540] Consistent with climate finance approaches to the climate commons, it thus provides a means of cyber-finance to stand alongside cyber-nuisance.[541] That is, cyber nuisance does not leave actors unable to shoulder the financial burden of upkeep out on their own.

Correlative rights further require that one not use cyberspace in a manner that is fundamentally inconsistent with its use and enjoyment by others. Hacks, malware, and similar intrusions are inherently suspect—such intrusions typically interfere with the privacy rights of participants and, as such, are internationally unlawful in their own right.[542] Cyber-nuisance adds an additional layer of protection by requiring correlative rights holders to diligently prevent conditions making such hacking more likely.

But the dissemination of content, too, can create a nuisance. Cyberbullying and cyberstalking are illustrative examples of conduct that can—in the right circumstances—be akin to the

---

536 *See infra* Section I.

537 TALLINN 2.0, *supra* note 22, at 84 r. 14.

538 Pierce, *supra* note 36 (discussing the concept of correlative rights in relation to property in oil and gas and in other contemporary issues).

539 Pierce, *supra* note 36.

540 Spur Indus., Inc. v. Del E. Webb Dev. Co., 494 P.2d 700, 708 (Ariz. 1972).

541 *See generally* ALEXANDER ZAHAR, CLIMATE CHANGE FINANCE AND INTERNATIONAL LAW (2017) (analyzing climate finance obligations of developed and developing countries).

542 *See generally* Sourgens, *Privacy*, *supra* note 290 (delineating a balancing test between reasonable expectations of privacy and the proportionality of the means used to intrude).

creation of, say, noise nuisances.[543] This means that cyber-nuisance does require policing of content beyond prohibiting intrusions through hacks.

Importantly, cyber-nuisance does not grant any cyber participant a veto right over others any more than nuisance gives people a veto right over their neighbor's conduct at home. If the point of cyber is connectivity, then there is a right to connect and exchange. This right entails that others may say things we find deeply offensive.[544] By analogy, cyber-nuisance addresses this concern by requiring a balancing of the respective rights of each participant.[545] It errs on the side of expression and only enjoins the *substantial* interference with the rights of others to use cyberspace that is, the balance must substantially favor intervention.[546]

In many instances, conduct is clearly a nuisance, and as such, requires abatement. The dissemination of revenge pornography is

---

[543] *See* Melissa Anne Springer, *Warning! Speak at Your Own Risk: First Amendment Restrictions on Off-Campus Physical, Emotional, or Cyberbullying*, 86 U. CIN. L. REV. 849, 863 (2018) (categorizing cyber conduct as a nuisance in ordinary language terms); Maureen E. Brady, *Property and Projection*, 133 HARV. L. REV. 1143, 1194-95 (2020) (discussing projecting images as nuisance when done with malicious intent and substantially interfering with the property right). Social media accounts are property. In re CTLI, LLC, 528 B.R. 359 (Bankr. S.D. Tex. 2015). As such, they are meaningfully analogous in important respects to the facades at issue in Professor Brady's article. This means that the ordinary language use of "nuisance" in the cyber context is in fact on to something. Cyber-bullying on social media accounts is an interference with a property interest. To the extent that it is substantial and unreasonable—and in fact malicious, per Professor Brady's discussion—the notion that it constitutes a nuisance is no longer far-fetched.

[544] In re CTLI, LLC, 528 B.R. 359, 371 (Bankr. S.D. Tex. 2015) (discussing the importance of connectivity and visibility in categorizing social media accounts as property); *see also* Brady, *supra* note 542, at 1202-13 (discussing the First Amendment implications of projections torts cases).

[545] *See* Springer, *supra* note 542, at 863; Brady, *supra* note 543, at 1202-13 (discussing the First Amendment implications of projections torts cases). The argument here is one of analogy.

[546] Crosstex N. Tex. Pipeline, L.P. v. Gardiner, 505 S.W.3d 580, 605 (Tex. 2016). The *Crosstex* case concerns interference with land. As discussed above in footnote 542, the substantial interference with a property interest is reasonably analogous to the substantial interference with a property interest *in land*. Particularly, the projection of images onto a house or business is in fact reasonably analogous to projecting on to a social media page in that it seeks to tag the person or business in a highly visible and identifiable manner. It is therefore reasonable to extend the nuisance logic here as well once the nature of social media as property takes further hold. I will develop this thought further in a future article.

one such instance.[547] Similarly, it is almost inherent in the name that the use of "troll farms" to amplify misinformation campaigns is a nuisance.[548] Troll farms amplify online noise to harm their target in the same way as the installation of industrial equipment in a residential neighborhood would. But the pendulum similarly swings in the other direction when it comes to the right of individuals to engage in conspiratorial discourse—even to trade in misinformation to make a political point. Free expression on the internet defies a truth police.

This shift away from a responsibility or fault paradigm has consequences for remedies, as well. The only listed potential self-help remedy for a nuisance is abatement. Self-help logically is similarly limited to the abatement logic.[549] The appropriate countermeasures (that is, self-help in the international context) for the failure of a State to respect correlative rights is also abatement. It is not a general countermeasure. It is a countermeasure that itself conserves the commons.

How then would cyber-nuisance treat the problems identified in Section II differently? The legal risk assessment of countering a potential outbreak of Emotet in Frankfurt illustrates the fault trap of *Tallinn 2.0*.[550] *Tallinn 2.0* created a negative incentive against preventing an outbreak.[551]

Cyber-nuisance creates the opposite incentive. First, correlative right holders have an overriding obligation to maintain the commons to the best of their ability. This includes an obligation to take reasonable preventive measures to render safe their portion of

---

[547] *See generally* Andrew Koppelman, *Revenge Pornography and First Amendment Exceptions*, 65 EMORY L.J. 661 (2016) (discussing freedom of expression and revenge pornography balancing in the First Amendment context).

[548] *See generally* Aja Romano, *Twitter released 9 million tweets from one Russian troll farm. Here's what we learned*, VOX (Oct. 19, 2018), https://www.vox.com/2018/10/19/17990946/twitter-russian-trolls-bots-election-tampering [https://perma.cc/GV43-PR3E] (reporting about the fake tweets created by a trollfarm in Russia during the 2016 U.S. election).

[549] *See Crosstex*, 505 S.W.3d at 610 ("It is well-settled that three different remedies are potentially available to a claimant who prevails on a private-nuisance claim: damages, injunctive relief, and self-help abatement").

[550] *See* Cimpanu, *supra* note 207.

[551] *See infra* Section III(c).

the commons.[552] The starting position therefore is different as *Tallinn 2.0* did not include such an obligation of prevention.[553]

Taking preventive measures in the cyber-nuisance context also helps to govern up. As discussed in the previous section, the nuisance principle is governed largely by neighborhood standards. Obligations are mutual.[554] This means that to benefit from greater efforts by others to maintain the commons, one therefore would be well-advised to lead by example and improve the commons. Such leading by example will not inure to one's detriment as one only is obligated to act as the neighborhood acts. Thus, if others fail to follow the lead, one should remain free to step back without falling below the threshold of neighborhood standards.[555] But if one succeeds, one benefits from the significantly increased cyber commons in much the same way as commons participants do in the water context—the improvement is exponential.

Cyber-nuisance thus lends itself to trust building. It allows neighbors to step up their respective efforts to improve the neighborhood. This effort creates a visible lift for others to follow suit. As a neighborhood principle, it further provides a greater incentive for networks to form in order to create better means to protect cyber and monitor and communicate about these efforts.

ii. The Attribution Shield

Cyber nuisance also helps to avoid the problems posed by the attribution for *Tallinn 2.0*. Briefly, the attribution problem meant that one had to prove that conduct in fact was perpetrated by an organ of state or that the state in fact had effective control over a cyber-operation.[556] This led to practical problems of proof that could easily become insurmountable.[557]

Cyber-nuisance shields from the attribution problem. It imposes an obligation on the State not to interfere substantially with the quiet

---

552 Derosne v. Puzin, D.P. [1845] I. 13, 14-15 (Fr.); *see* Zile, *supra* note 380, at 294-98 (translating and analyzing the relevant positions of the Derosne v. Puzin in English.).

553 TALLINN 2.0, *supra* note 22, at 43-44 r. 7 ¶¶ 7-8.

554 *See* Negbi, *supra* note 487, at 828.

555 CHAMOULAUD-TRAPIERS, *supra* note 389, at 167.

556 TALLINN 2.0, *supra* note 22, at 87, 94 rr. 15 & 17.

557 *See infra* Section II.

enjoyment of others. The threshold for this obligation is lower than the attribution threshold for conduct the State supports, whether directly or indirectly. Further, this obligation also entails an obligation to harden infrastructure so as to make it more difficult for third parties to use State capabilities to further a cyber-operation by third parties.

The first problem concerned attributing the hack of South Korean banks as well as Sony to North Korea. As discussed above, it is not entirely clear whether the initial identification of North Korea as the culprit in these attacks was premised upon sufficient evidence.[558] A cyber-nuisance paradigm would sidestep this problem. It would instead require efforts by North Korea to avoid incursion into its cyber network. Notably, North Korea would not have to achieve this end alone. Rather, those interested in requiring North Korea to avoid future abuse of its cyber infrastructure under a cyber-nuisance approach may well be asked to help pay for the upgrade.[559] But to the extent that North Korea's infrastructure is below the threshold of other similarly situated actors, cyber nuisance can require that its infrastructure be further improved.

The second problem discussed above concerned "patriotic hackers."[560] Patriotic hackers presented a problem for *Tallinn 2.0* as they are not state organs and are not under the effective control of the State. Cyber nuisance would impose multiple obligations on the State, each of which would likely make patriotic hackers a less palatable scenario for cyber operations.

First, the State could very well be made liable for "arming" or supporting patriotic hackers. It is reasonably clear even under an intentional nuisance view that the kind of support given to such

---

[558] Brian Todd & Ben Brumfield, *supra* note 173.

[559] Spur Indus., Inc. v. Del E. Webb Dev. Co., 494 P.2d 700, 708 (Ariz. 1972). The *Spur Industries* case is one of the leading cases for this type of remedial approach in U.S. law. *See* Osborne M. Reynolds Jr., *Of Time and Feedlots: The Effect of Spur Industries on Nuisance Law*, 41 WASH. U. J. URB. & CONTEMP. L. 75 (1992). This remedial logic applies by analogy to the international setting if we follow a nuisance logic. In the international setting, such an approach is already in ascendency in the context of another area of law that is frequently associated with commons governance—namely, climate in the context of climate finance obligations to support carbon mitigation efforts by developing countries. *See* ZAHAR, *supra* note 541 (discussing climate finance); Scott J. Shackelford, *The Future of Frontiers*, 23 LEWIS & CLARK L. REV. 1331, 1372-74 (2020) (discussing climate change and cyber from a commons governance perspective); Frederic G. Sourgens, *A Parisian Consensus*, 60 COLUMB. J. TRANSNAT'L L. (forthcoming, 2021) (discussing climate change from an energy commons governance perspective).

[560] Calamur, *supra* note 185.

groups would make it materially likely that harm will befall somebody whom the patriotic hacker believes to represent a threat to the fatherland.[561] To support such persons in their endeavors therefore would not be consistent with the cyber nuisance paradigm.

Second, if the State is made responsible for the interference with the rights of third parties by actors it cannot effectively control, it is all the more likely that the State will wish to bring such capabilities in house. Such a move would be prudent if only to have greater operational control. And control now is no longer a hallmark for fault trigger.

At the same time, the standard remains heavily contextual. A State therefore only has cause to complain about the conduct of another if it is not itself engaged in the same kind of activity. The more espionage and other activities States conduct, the less credible a claim for cyber-nuisance by such a State becomes. Given the cyber operations loosely said to be affiliated with most (even regional) powers, cyber-nuisance would require mutual cyber disarmament before any claim would lie for violation of one's correlative rights. An abuser of rights cannot complain of abuse of rights.

The attribution shield is the first step in removing an obstacle to good commons governance. This obstacle is the incentive structure of a hierarchically privileged State able to provide rewards to those unaffiliated with it to achieve certain goals no matter the collateral damage.[562] This incentive structure is indicative of failed commons governance mechanisms and is a kind of polycentricity of decay.[563] It erodes trust and creates incentives to emulate destructive behaviors. And yet, the erosion of trust is diffuse and networked between *realpolitik*-driven State actors and their collaborators. Removing this shield is therefore instrumental in securing a long-term sustainable governance process.

---

[561] Crosstex N. Tex. Pipeline, L.P. v. Gardiner, 505 S.W.3d 580, 605 (Tex. 2016). Again, the reference to *Crosstex* is intended by analogy as *Crosstex* is a sophisticated articulation of nuisance law principles – principles which this Article has argued in fact enjoy the status of a general principle of law. The logic of that principle therefore should be applicable – by analogy – in the international setting.

[562] *See generally* OSTROM, *supra* note 32, at 157-73 (illustrating irrigation development projects in Sri Lanka).

[563] *See* OSTROM, *supra* note 32, at 157-73.

iii. Polycentric Connectivity

The final problem for *Tallinn 2.0* highlighted in the first section was its State-centered approach and the loss of core non-State stakeholders in cyber governance. *Tallinn 2.0* is adamant that it applies only to State conduct.[564] It further did not provide a seamless, nestled governance structure by allowing States to not preventively regulate, to not harden their cyber infrastructure, and to not monitor cyber conduct in their respective jurisdictions.[565]

Cyber-nuisance changes this approach to cyber-governance radically. Cyber-nuisance requires States to respect the correlative rights of all participants in cyberspace. Cyber-nuisance takes States to task to use their regulatory power to bring about this result and thus imposes a regulatory obligation on the State preventively to regulate, harden cyber infrastructure, and monitor cyber conduct in a manner consistent with the overall neighborhood standards in the relevant portion of cyberspace.

Furthermore, cyber-nuisance takes into account the input from non-State actors as very real parts of the obligations involved. The cyber neighborhood is not just the State-owned infrastructure. It includes cyberspace as a whole. The standard of conduct of private actors in cyber therefore are an integral part of setting neighborhood expectations. Thus, if the private actors in cyber collectively raise the standard of cyber protection, the State would in principle be required to follow suit under a nuisance logic. The far more likely outcome, however, is that these actors will interconnect and exchange on governance and thus share in respective governance responsibilities under a cyber-nuisance paradigm.

Moreover, the discussion above on regulating cyber speech already suggests that the appropriate balancing will not depend upon state actors alone. If posts on Twitter or Facebook constituted a cyber-nuisance, it would require Twitter or Facebook to assist in regulating this conduct, for instance, by taking down the posts.[566] Twitter and Facebook presumably will respond to regulatory

---

564 TALLINN 2.0, *supra* note 22, at 17 r. 4.

565 *See infra* Section III(a).

566 *See generally* Jessica Guynn, *These are Facebook's secret rules for removing posts*, USA TODAY (Apr. 24, 2018, 2:24 PM ET), https://www.usatoday.com/story/tech/news/2018/04/24/facebook-discloses-secret-guidelines-policing-content-introduces-appeals/544046002/ [https://perma.cc/X9XK-CGYD] (describing the rules and guidelines on permissible and impermissible posts that Facebook published in 2018).

pressures to do so. They will also respond to market pressures to do so.[567] But in the final analysis, the abatement of the nuisance—and the setting of the first line of standards to avoid nuisances—will lie with apex platforms.

This point is sadly no longer exclusively academic. Following the attack on the U.S. Capitol by supporters of then-President Trump on January 6, 2020, social media platforms such as Twitter did the previously unthinkable—they "de-platformed" the President of the United States; that is, they terminated his ability to post to the network.[568] Other actors, such as Amazon, then cut off the ability of other platforms, like Parler, to operate.[569] These actions—by private companies arguably in keeping with their respective terms of use—represent a very tangible attempt to abate a cyber-nuisance: to shut off the use of cyberspace as a means to plan violent attacks on lawmakers and government institutions ahead of the inauguration of President Biden.[570]

The cyber-nuisance perspective allows a different lens through which to assess the actions of social media platforms. This lens would suggest that as long as there is a real threat, premised in actionable intelligence, that cyber platforms are indeed used to plot violence, the abatement logic suggests even such drastic action. The fact that private actors do in fact take such action thus is consistent with a cyber-nuisance paradigm.

At the same time, the cyber-nuisance paradigm suggests that there must be clear limits to such de-platforming. Consider the military coup in Myanmar on February 1, 2021. The *New York Times* reported that "[m]obile networks and the internet were intermittently down in major cities, and some local journalists went

---

567 *See* Mike Isaac, *Why Everyone Is Angry at Facebook Over Its Political Ads Policy*, N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/technology/campaigns-pressure-facebook-political-ads.html [https://perma.cc/RX3G-9SP2].

568 *See* Dylan Byers, *How Facebook and Twitter decided to take down Trump's accounts*, NBC NEWS (Jan. 14, 2021, 5:01 PM EST), https://www.nbcnews.com/tech/tech-news/how-facebook-twitter-decided-take-down-trump-s-accounts-n1254317 [https://perma.cc/8TZB-LDHB].

569 *See* Russell Brandom, *These are the violent threats that made Amazon drop Parler*, THE VERGE (Jan. 13, 2021, 10:17 AM EST), https://www.theverge.com/2021/1/13/22228675/amazon-parler-takedown-violent-threats-moderation-content-free-speech [https://perma.cc/P6RB-N5Z2].

570 *See* Jon Brodkin, *Parler's attempt to get back on Amazon Web Services rejected by judge*, ARS TECHNICA (Jan. 21, 2021, 5:30 PM), https://arstechnica.com/tech-policy/2021/01/judge-rejects-parler-claim-that-amazon-must-reinstate-web-hosting-service/ [https://perma.cc/4Z7R-9SK3].

into hiding for fear that their reporting could compromise their safety."[571] Similarly, one of the flashpoints in Hong Kong's protests was the use of social media to "galvanize support during a political movement."[572] In fact, such social media posts led to arrests under Hong Kong's new national security law as inciting secession.[573] Amnesty International has called out this conduct by the Chinese government as fundamentally inconsistent with the right to free expression, noting that "[i]nternational human rights laws do not allow states to restrict all peaceful expression in the name of national security."[574] This rationale obviously applies to arrests in the name of national security.[575] But it should also extend to *access* to cyber connectivity and the ability to engage in peaceful expression in the first place.

If such conduct by states is questionable because it limits freedom of expression and connectivity, cyber-nuisance suggests that it should similarly be problematic when it is perpetrated by private apex actors. The correlative rights of cyber participants are impaired by *both*, state action and private action. The cyber-nuisance logic, therefore, requires some limitation on the power of apex platforms to shut out those with whom it disagrees.

Here, the currently unfolding reaction to the January 6 Capitol riot will provide an early test case.[576] The abatement strategy by apex platforms to deprive certain kind of speech of a platform can be justified.[577] The Amnesty International critique of Chinese

---

571 *See* Hannah Beech, *Myanmar's Leader, Daw Aung San Suu Kyi, Is Detained Amid Coup*, N.Y. TIMES (Jan. 31, 2021), https://www.nytimes.com/2021/01/31/world/asia/myanmar-coup-aung-san-suu-kyi.html [https://perma.cc/L2GR-7663].

572 *See* Grace Shao, *Social media has become a battleground in Hong Kong's protests*, CNBC (Aug. 16, 2019, 5:41 PM EST), https://www.cnbc.com/2019/08/16/social-media-has-become-a-battleground-in-hong-kongs-protests.html [https://perma.cc/4ZAW-68L7].

573 *See* Amnesty Int'l, *Hong Kong: National security arrests over social media posts violate freedom of expression* (July 30, 2020, 14:20 UTC), https://www.amnesty.org/en/latest/news/2020/07/hong-kong-national-security-arrests-over-social-media-posts-violate-freedom-of-expression/ [https://perma.cc/K8JF-VQMM].

574 *Id.*

575 *Id.*

576 *See* Adam Satariano, *After Barring Trump, Facebook and Twitter Face Scrutiny About Inaction Abroad*, N.Y. TIMES (Jan. 14, 2021), https://www.nytimes.com/2021/01/14/technology/trump-facebook-twitter.html [https://perma.cc/V77A-B9HX].

577 *Id.*

crackdowns in the name of national security here is instructive: is the speech in question "peaceful expression?"[578] Incitement to violence certainly is not.[579]

The actions of apex platforms become increasingly problematic if the platforms use their market power in the absence of such a threat of violence. The Biden White House Press Secretary Jen Psaki bluntly stated that the Biden White House does not miss President Trump on Twitter.[580] As that statement suggests, this inability is beginning to affect political discourse. The line between policing dangerous content and peaceful expression therefore appears increasingly tenuous to hold.

Cyber-nuisance would therefore counsel that de-platforming is an acceptable abatement only to a point. Once actionable threats of violence have ceased, continuing to shut out cyber participants on the basis of the content of their speech is problematic. In fact, de-platforming might even give rise to a cyber-nuisance in its own right as it infringes on the correlative rights of a large number of peaceful actors.[581] How apex platforms strike this balance at the current time, therefore, will be of particular importance to watch.

Radical though this change is, it does not give up the function of cyber-nuisance as a principle of international law, that is, the law between States. Cyber-nuisance as a principle of international law does not bind non-State actors as such.[582] Rather, cyber-nuisance as a principle of international law requires States to communicate with non-State actors under their jurisdiction to regulate in a manner consistent with the correlative rights of other States and other non-State cyber participants.

But importantly, cyber-nuisance functions as more than just a principle of international law. It also has a role to play in transnational and domestic law. Thus, if the submission in this Article is right, non-State actors are themselves subject to cyber-

---

578 *See* Amnesty Int'l, *supra* note 573.

579 *See* Satariano, *supra* note 576.

580 *See* Jonathan Easley, *Psaki: We don't miss Trump on Twitter*, THE HILL (Feb. 1, 2021, 01:29 PM EST), https://thehill.com/homenews/administration/536783-psaki-we-dont-miss-trump-on-twitter [https://perma.cc/4UR6-JWY9].

581 The argument that parties have consented to the power of apex platform to use their market power in this way is the subject of a future article. As I will argue, the one-sided fundamental alteration of the marketplace does not fall within the scope of such consent, even if it is arguably included in the terms of use as its deployment by apex platforms would not be in good faith.

582 *See* CRAWFORD 2014, *supra* note 96, at 221 (discussing the traditional scope of application of international law).

nuisance concerns as a holder of correlative rights and correlative duties vis-à-vis other, similarly situated non-State actors. These correlative rights and duties are part of the legal decision-making process of these non-State actors as part of their own governance environment.

This means that cyber sets up nestled governance processes that all follow a similar logic of correlative rights as made actionable in the nuisance context. States act in a regulatory and a sovereign capacity as actors in cyber in their own right as guided by the State-based public international law cyber-nuisance principle. Global business transactions concerning cyber infrastructure are governed by the transnational principle of cyber-nuisance as incorporated in the *lex digitalis*. And the relationship between consumers or users of cyber and private companies in turn is governed by correlative rights principles as established in their domestic laws.

Each of these cyber-nuisance processes sits nestled in the other as each can affect the other.[583] An increase in cyber-diligence in the transnational space will affect neighborhood conditions in the international setting. International diligence obligations will change the domestic regulatory space. The domestic regulatory space will affect the transnational space and so on. Governance is thus truly polycentric. Cyber-nuisance can bring all stakeholders to the table to govern up.

This leaves the question of how a cyber-nuisance paradigm would look at NotPetya.[584] We already have the lion share of the answer to this problem. To begin with, a cyber-nuisance paradigm would flag that many actors failed to do their part to protect the commons and thus, the correlative rights of other participants. The development of EternalBlue by the NSA would raise a flag as the program foreseeably could have been used to wreak precisely the havoc that it did.[585] The hack of EternalBlue and its dissemination also would raise additional cyber-nuisance concerns.[586] Leaving aside the legality of the deployment of NotPetya in Ukraine itself, the willingness to do collateral damage globally would be a further concern.[587] Finally, business would have a role to play—Windows

---

583 *See* OSTROM DIVERSITY, *supra* note 32, at 269-70.

584 *See* Greenberg, *supra* note 121.

585 *See* Greenberg, *supra* note 121.

586 *See* Greenberg, *supra* note 121.

587 *See* Greenberg, *supra* note 121.

in dealing with a vulnerability and global business in protecting critical infrastructure from cross-company contamination.[588]

In the case of NotPetya, cyber-nuisance would not be a good tool to assign blame. Given the chain reaction needed to lead to NotPetya, cyber-nuisance would be of reasonably little help in a liability context. Maersk and consequently Denmark would have a right to act against the Russian Federation if the NotPetya attack could be attributed to the Russian Federation. But they likely would have had such a right under *Tallinn 2.0,* in any event.[589] The more interesting question is whether Maersk and consequently Denmark would have rights against the United States and Ukraine—rights they would not have under *Tallinn 2.0*.[590] While cyber-nuisance provides a plausible articulation of how the United States and Ukraine created conditions causing Maersk a substantial impairment of its correlative rights in cyber, it is far from clear whether such arguments would clear the hurdles of causation and overcome Maersk's own conduct and the relative reasons by the United States and Ukraine, for their respective actions and omissions would not ultimately speak against imposing liability on a cyber-nuisance theory.

But the point of cyber-nuisance is precisely not to assign blame but to assist in future decision-making.[591] And here, cyber-nuisance is both far more robust and far more consistent with the actual regulatory response to NotPetya. It turns out that the United States and its Department of Homeland Security has stepped up its regulatory dialogue businesses to prevent similar vulnerabilities by issuing guidelines and discussing their implementation with businesses.[592] Companies on their own are acting to harden their own cyber defenses.[593] In other words, actors are responding as prudent correlative rights holders both to protect themselves and the commons. Such collaborative action between States and

---

588 *See* Greenberg, *supra* note 121.

589 *See* Piret Pernik, *Responding to "the Most Destructive and Costly Cyberattack in History*," RKK-ICDS (Feb. 23, 2018), https://icds.ee/responding-to-the-most-destructive-and-costly-cyberattack-in-history/ [https://perma.cc/JX7C-7HNP].

590 *Id.*

591 *See* REISMAN, *supra* note 152, at 183-90.

592 *See* NAT. GAS COUNCIL, DEFENSE IN DEPTH: CYBER-SECURITY IN THE NATURAL GAS & OIL INDUSTRY (2018) https://www.api.org/~/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf [https://perma.cc/MK7E-TUHM].

593 *Id.*

businesses increases neighborhood standards. This increase in neighborhood standards in turn lays the predicate for future appraisal of new threat scenarios—and it is perfectly consistent with the decision by City of Frankfurt to shut down its IT department in the face of an Emotet threat to avoid a cross-contamination.[594]

In other words, many actors are already engaging each other in cyber in a manner that is consistent with the concept of correlative rights and nuisance as developed in this Article. Cyber-nuisance would provide a better rubric through which to understand this conduct and guide it more quickly towards a better maintained, more diffusively governed cyber commons.

The SolarWinds hack showcases why accelerating this process is so important. SolarWinds has shown us both the promise and peril of a cyberspace that is fundamentally co-operated by public and private entities. On the side of peril, it was the lax security at a globally operating apex cyber company that permitted the spectacular hack to come off in the first place.[595] It was the strategic importance of this company to governmental infrastructure that allowed the hack to elude early detection—and "exploit[] seams in U.S. defenses."[596] Public and private cybersecurity, therefore, are fused at the hip and must be treated as such to protect the commons.

But just as importantly—and here is the promise of the current paradigm—it was a private company and not the government that discovered the intrusion and began the process of analyzing the breach.[597] The fact that actors collaborate across the public/private divide to secure the commons therefore is instrumental to hardening cyber-defenses and securing greater access to the promise of cyber. It is only when such cooperation intensifies that rogue actors (be they state controlled, commercial, criminal, or in the grey between) can be found out and the consequences of their conduct abated. In other words, while there is a path, there is a long way yet to travel.

VI. CONCLUSION: CYBER-NUISANCE AND CYBER-GOVERNANCE

What are the consequences of cyber-nuisance for cyber-governance? Cyber-nuisance has made several significant

---

594 *See* Cimpanu, *supra* note 207.

595 *See* Sanger, *supra* note 20.

596 *See* Sanger, *supra* note 20.

597 *See* Sanger, *supra* note 20.

contributions to cyber governance. The first of these contributions, while it may appear reasonably minor, is paradigm-shifting. *Tallinn 2.0* rejected to treat cyber as a commons on the grounds that cyber is subject to the jurisdiction of States and as such not communally owned.[598] The Article has shown that this is a significant misunderstanding of commons and commons governance and should lead the *Tallinn 2.0* experts to rethink their conclusion.

Centrally, *Tallinn 2.0* starts out from the principles of sovereignty that each State shall be absolutely free to enjoy its own rights within its sovereign jurisdiction and that each State may not unreasonably interfere with the rights of States in their respective jurisdictions.[599] This articulation of the starting point in *Tallinn 2.0* is close to a textbook Roman law understanding of property.[600] It also mirrors the understanding of otherwise apparently absolute property rights in the common law.[601]

What this Article has shown is that commons form when these absolute rights interact with each other to exploit a common pooled resource and create correlative rights for its participants. In the Roman law, this understanding gave rise to the *actio negatoria*.[602] At common law, it gave rise to the action of nuisance and later to a fully fleshed understanding of correlative rights the protection of which remains actionable in nuisance.[603]

The point that can hardly be overstressed is this: oil and gas lessees have a property right in fee simple determinable in the mineral estate.[604] This right is in fee.[605] This is similar to the sovereign concern in *Tallinn 2.0*.[606] The fact that oil and gas lessees producing from a common formation are nevertheless acting in a commons and are correlative rights holder in that commons should put to the rest the notion that absolute ownership of a part defeats the existence of a commons in a whole or correlative rights against

---

598 TALLINN 2.0, *supra* note 22, at 11.

599 TALLINN 2.0, *supra* note 22, at 13, 16-17.

600 *See* Mellius De Villiers, *Nuisances in Roman Law*, 13 L.Q. REV. 387, 391 (1897).

601 *See* Pierce, *supra* note 36.

602 *See* PETIT, *supra* note 420, at 703-04.

603 *See* Pierce, *supra* note 36, at 259-64; Fraley, *supra* note 327, at 453-57.

604 *See* Porter Wright, *What is an Oil and Gas Lease?*, OIL & GAS L. REP. (Sept. 27, 2013), https://www.oilandgaslawreport.com/2013/09/27/what-is-an-oil-and-gas-lease-a-federal-court-in-ohio-predicts-ohio-law/ [https://perma.cc/2E39-9LMP].

605 *Id.*

606 TALLINN 2.0, *supra* note 22, at 13, 16-17.

other commons participants.[607] And this is not a quirk of American property law. It is the received wisdom of Justinian.[608] Moreover, it is consistent with legal traditions as diverse as *shari'a*, the mixed jurisdiction of Israel, and the People's Republic of China.[609]

This alone requires a fundamental rethinking of *Tallinn 2.0*. It completely misses from view that commons create correlative rights.[610] A legal decision-making toolkit operating in a commons that does not account for correlative rights is flawed and significantly under-protects the rights of participants in the commons. Not only that, but it also threatens the very infrastructure *Tallinn 2.0* seeks to protect. As property (sovereignty) matters to *Tallinn 2.0*, so should the commons.

Importantly, *Tallinn 2.0* hints at the critical importance of such a commons understanding of cyber when it imports the core diligence norm from international environmental law.[611] It just misunderstands it. The diligence norm in international environmental law developed in jurisprudence from *Trail Smelter* onwards is a nuisance norm to protect U.S. communities against cross-boundary air pollution from Canadian smokestacks.[612] It imports precisely the commons concerns *Tallinn 2.0* rejects.[613]

Tallinn 2.0, in other words, mistranslates the general international law it wishes to import into cyber. Cyber-nuisance sets out how a more faithful translation would change the landscape of cyber governance in the mold of *Tallinn 2.0*. Such a translation would allow for a more networked approach to cyber-security. It further would provide a means to move away from a view of cyber as the new battlefield and towards an understanding of cyber as a space of correlative rights and cooperative collaboration.

This focus on correlative rights can also banish the threat of spiraling countermeasures wreaking further destruction on cyber. The avowed reason to set a high threshold for diligence obligations was to avoid a scenario in which States impose ever harsher countermeasures on each other for a failure to keep their diligence

---

607 *See* Pierce, *supra* note 36.

608 *See* De Villiers, *supra* note 600, at 391.

609 *See infra* Section V.B.

610 *See* Pierce, *supra* note 36.

611 TALLINN 2.0, *supra* note 22, at 35.

612 *See* Trail Smelter Case (U.S. v. Canada), III UNRIAA 1905, 1925 (Apr. 16, 1938 & Mar. 11, 1941); *see also* PHILIPPE SANDS & JACQUELINE PEEL, PRINCIPLES OF INTERNATIONAL ENVIRONMENTAL LAW 25, 254 (4th ed. 2018).

613 TALLINN 2.0, *supra* note 22, at 11.

obligations. This reason makes sense in a responsibility paradigm. It is out of place in a correlative right paradigm.

Cyber-nuisance has shown that the appropriate remedy for the substantial impairment of correlative rights is abatement.[614] Self-help or countermeasures therefore in the first instance are also limited to actions in abatement, that is, actions that remove the specific cyber threat.[615] This limitation already excludes the tit-for-tat of spiraling countermeasures.[616] To constitute permissible self-help, the nuisance paradigm requires that each countermeasure be specifically tailored to abate the nuisance.

This still leaves significant room for cyber operations, including offensive cyber operations. A State that stands to suffer particular harm (in other words, would have standing to sue for a private nuisance) may take countermeasures to seek out and destroy cyber capabilities of States and non-State actors alike to the extent that those cyber capabilities demonstrably and substantially threaten its correlative rights to enjoy the cyber commons. To do so, it must warn the relevant actors to give them an opportunity to abate the nuisance themselves, consistent with existing countermeasure principles.[617] If the warning goes unheeded, the State could then act to protect the cyber infrastructure.[618] But to act in such defense of the commons in logic would also require the State to forswear the development and deployment of similar capabilities to those being sought and destroyed. Estoppel would require as much.[619]

To the extent that such measures cannot be taken directly, indirect countermeasures may still be permissible in very limited circumstances. Specifically, if any attempt at abatement would itself harm the cyber commons, this would preclude the use of those countermeasures. Then, other measures may well be necessary to bring about abatement. Even then, however, the logic of the regime set out in this Article suggests that any actions may not themselves create a cyber-nuisance. And any such actions must be preceded by appropriate offers of assistance to abate the cyber nuisance proportionate to the countermeasures about to be undertaken to

---

614 *See Crosstex*, 505 S.W.3d at 610; TUNC, *supra* note 381, at 56; Barak, *supra* note 478, at 694 (discussing *Ata Textiles Co.*, (1976) 30(iii) P.D. 785 (Isr.)).

615 *See Crosstex*, 505 S.W.3d at 610; CHENG, *supra* note 282, at 97-100.

616 *See* Jensen & Watts, *supra* note 26, at 1563-64.

617 ILC Articles, *supra* note 57, at 135.

618 ILC Articles, *supra* note 57, at 135.

619 *See* CHENG, *supra* note 282, at 143-44.

comply with the requirement to warn as adapted to its new environment.[620]

This remedial consequence of the cyber-nuisance paradigm allows one to have both greater diligence and less chaos from sprawling cyber countermeasures.[621] It again makes States and other participants in cyber accountable to each other for the conservation of their commons. At worst, the remedial consequence of excessive self-help would lead to excessive conservation. This result is broadly consistent with the correlative rights rationale to put sustainability of use for all above the interests of use of each.[622] It is therefore not an unintended consequence or crude destabilizer of the commons.

Finally, cyber-nuisance also begins to provide the clues to answer that has vexed the discussion from the other, private law side. As discussed in the previous section, transnational lawyers previously insisted upon the existence of a transnational *lex digitalis*.[623] This insistence upon a *lex digitalis* was premised upon the idea that cyberspace is beyond the jurisdiction of a States to regulate—that it is a communally owned space in needed of truly stateless regulation.[624]

Cyber-nuisance has suggested that this insistence is just as wrong as the insistence by *Tallinn 2.0* that cyber is not a commons. The *lex digitalis* went too far in completely unmooring cyber from the underlying jurisdictional ties that bind it to the brick-and-mortar world. It turns out that it may have done so on the basis of the same misunderstanding as *Tallinn 2.0*, but in reverse, namely on the basis of the assumption that a commons must be a fully communally owned space.[625] As the comparative property law analysis in this Article has shown, this premise is simply false. Commons can exist *between* and *across* distinct and parceled out claims of ownership—or in the sovereign context, jurisdiction. What makes such commons interesting is that the relative ownership claims strengthen rather than weaken the correlative rights involved. It provides a stronger anchor for the holding of correlative rights and thus provides a more

---

620 ILC Articles, s*upra* note 57, at 135.

621 *See* Jensen & Watts, *supra* note 26, at 1563-64 (raising the countermeasures threat as a reason against increased diligence requirements).

622 *See* OSTROM, *supra* note 32, at 108-42.

623 *See, e.g.*, Michaels, *Pluralism*, *supra* note 298, at 247.

624 Michaels, *Pluralism*, *supra* note 298, at 247.

625 Michaels, *Pluralism*, *supra* note 298, at 247.

interesting conception of commons governance in a co-owned relationship between separately owned spaces.

This understanding is likely to provide a more interesting intersect between the State-based world of *Tallinn 2.0* and the stateless world of the *lex digitalis*. Cyber-nuisance thus can function as a bridge between normative orders that can doubtless enrich each other through the understanding of the respective "other half" they currently miss.

Cyber-nuisance finally reinvigorates the etymological pull of cyber. The κυβερνάτας of a Greek vessel was its steersman or guide.[626] Steering a vessel is not a question of land or open sea. It requires both. This was anchored in the very soul of the seafaring Athenian. Just ask an Athenian about their founding myths and they would tell you their ancestors were sprung from the land of Attica itself, *autochthones*.[627] The greatest seafarers of the ancient West—the greatest steersmen—were thus earthborn and seaborne alike. Land and sea, land and commons, were no contradiction—they were part of the same identity. Cyber, and correlative rights in cyber, reflect the same experience 3,400 years hence.

---

[626] Κυβερνήτης, MIDDLE LIDDELL LEXICON, http://www.perseus.tufts.edu/hopper/morph?l=kuberna%2Ftas&la=greek&can=kuberna%2Ftas0&prior=kube/rnasis#lexicon [https://perma.cc/UDD9-TLVP]. For a fuller discussion of the historical root and usage of the term and how it came to be associated with cyberspace, see *The Vocabularist: How We Use the Word Cyber*, BBC (Mar. 15, 2016), https://www.bbc.com/news/magazine-35765276 [https://perma.cc/926Z-LT6S]. For a further interesting etymological link from Κυβερνήτης to the English governor, see James William Johnson, *"Reverend Shapes:" Lord Rochester's Many Mentors*, *in* MENTORING IN EIGHTEENTH-CENTURY BRITISH LITERATURE AND CULTURE 17, 17 (Anthony W. Lee ed., 2010).

[627] For a discussion of this myth, see Vincent J. Rosivach, *Autochthony and the Athenians*, 37 CLASSICAL Q. 294 (1987).