"Of Hacking and Human Rights:
Designing the International Attribution Rules"

Leslie Johns
Associate Professor of Political Science and Law
UCLA
ljohns@polisci.ucla.edu

Francesca Parente
Postdoctoral Fellow
Princeton University
fparente@ucla.edu

15 August 2019

Abstract

Cyberattacks pose a grave threat to states, but many prominent attacks go unpunished under international law, in part because attacks carried out by individual 'hacktivists' are not attributable to states. Attribution rules under the *lex generalis* on state responsibility – which covers cyberattacks – contain multiple disconnects between legal breaches and punishments. However, many specialized areas of law depart from this approach. What explains this variation? We argue that to understand the existing and potential design of attribution rules, we must understand why states are tempted to break international law. In this paper, we describe three competing political theories of why states break international law (enforcement, managerial, and flexibility). We then elucidate the implications of each of these theories for how states design rules for attribution. We argue that the general attribution rules accommodate managerial and flexibility concerns, but neglect the competing objective of enforcement. We then argue that when states prioritize enforcement, they should design specialized rules. We demonstrate the plausibility of our approach by examining case-law from the Inter-American Court of Human Rights, which differs from the general rules on attribution that are used by other institutions and areas of law. Without stronger rules that make the conduct of 'hacktivists' attributable to states, it may be difficult—if not impossible—to adequately counter the dangers posed by cyber threats.

1 Introduction

In spring 2007, a sixty-year-old statue started a virtual 'war.' At the end of the Second World War, Soviet soldiers expelled German Nazi forces from Tallinn, Estonia, a small city on the coast of the Baltic Sea. In celebration of this event, the Soviet Army created a war memorial called the 'Monument to the Liberators of Tallinn' with a Bronze Soldier statue standing watch over the unclaimed bodies of Soviet soldiers. After the fall of the Soviet Union in 1989, Estonia gained its independence and gradually realigned itself with western Europe. Consequently, the Estonian government decided to relocate the Bronze Soldier statue and the unclaimed bodies of Russian soldiers from their prominent position in the center of Tallinn to a military cemetery on the edge of the city. This move generated widespread criticism by Estonia's ethnic Russian community. In addition to large conventional protests, 'hacktivists'—political activists who use computer networks for subversive purposes—launched massive cyberattacks on the websites of Estonian government agencies, news organizations, and private businesses.

During and after the attacks, the Estonian government and numerous intelligence and technology experts blamed Russia for inciting and supporting the attacks. Merit Kopli, the editor of a major Estonian newspaper that was targeted in the attack, declared: 'The cyber-attacks are from Russia. There is no question. It's political.'[1] Anonymous NATO officials told western news sources that the attacks were probably not the work of isolated individuals. They believed that the depth and sophistication of the operations indicated that Russian security services were involved.[2] NATO legal experts concluded that if such attacks were committed by a state, they would constitute an illegal intervention.[3] But was Russia legally responsible for the attacks? The NATO experts found it

[1] Quoted in Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian,* 16 May 2007.
[2] Traynor, 'Russia accused.'
[3] Michael N. Schmitt, *Tallinn Manual 2.0 on the international law applicable to cyber operations* (Cambridge: Cambridge University Press, 2017). See also Rex Hughes, 'A treaty for cyberspace',

was not because 'there is no definitive evidence that the hacktivists … operated pursuant to instructions from any State, nor did any State endorse and adopt the conduct.'[4] The cyber-attacks were thus the work of individuals rather than of states.

Two years later, the Inter-American Court of Human Rights (IACHR) was confronted with a similar challenge: it needed to determine whether a human rights violation by an individual could be attributed to a state. The case involved the murder of Blanca Jeannette Kawas Fernández, a prominent environmental activist. Honduras claimed that it was not responsible because Kawas Fernández had been killed by private individuals who were unaffiliated with the state. However, the IACHR argued that Honduras was responsible for violating Kawas Fernández's right to life because it had failed to investigate her murder; this entailed 'in some way, assist[ance] by public authorities, which would entail international responsibility for the State.'[5] This reasoning stands in stark contrast to the legal rule used by NATO officials: that state instructions or endorsement are necessary for the conduct of private individuals to become conduct of a state.

Why did the NATO experts and the IACHR come to such different conclusions? In other words, why were the actions of human rights violators attributable to a state, while the actions of hackers were not? One will note, of course, that different rules applied in each case. NATO experts based their opinion on the general rules on state responsibility, which have stricter requirements for attributing acts of individuals to the state. In contrast, the IACHR used its own jurisprudence, where the attribution standard is lower. Each set of legal experts followed their own rules. However, if the IACHR had applied general rules of state responsibility, it would not have found Honduras responsible because the murder was committed by private actors that the state did not control. But why were the attribution rules designed differently in the first place?

International Affairs 86, 2010, pp. 523-541; and David S. Yost, 'NATO's evolving purposes and the next Strategic Concept', *International Affairs* 86, 2010, pp. 489-522.

[4] Schmitt, *Tallinn Manual*, p. 382.

[5] IACHR, *Kawas Fernández v. Honduras* (2009), para. 78.

This question—of when states are legally responsible for the acts of individuals—has immense importance for contemporary cybersecurity. The 2007 attack on Estonia was not a unique example. Many states—including China, Iran, North Korea, and Russia—have been widely accused of either sponsoring or condoning cyberattacks by private actors for national security reasons.[6] State victims of major cyberattacks with political objectives now include France, Georgia, Indonesia, Japan, Kosovo, Mexico, and the US.[7] How can we explain the relatively weak attribution rules for cybersecurity when attribution rules are much stronger for other issues, like human rights?

We argue that to understand the design of international law for attribution, we must understand why states sometimes break international law. We describe three competing political theories—the enforcement, managerial, and flexibility perspectives—with different assumptions and implications about legal design. We argue that general rules (*lex generalis*) of state responsibility on attribution match the concerns of the managerial and flexibility perspectives, but neglect the enforcement perspective. However, when states strongly support a legal regime, they can and should re-prioritize enforcement by developing specialized rules (*lex specialis*) on state responsibility to better promote their common objectives. Without stronger rules that make the conduct of 'hacktivists' attributable to states, it may be difficult—if not impossible—to adequately counter the dangers posed by cyber threats.

To demonstrate the feasibility of this option, we discuss state responsibility rules in the IACHR. This institution has departed from the *lex generalis* by adopting progressively more muscular standards to hold states accountable for past breaches and prevent future breaches. In our conclusion, we return to the issues raised in the 2007 cyberattacks on Estonia and *Kawas Fernández v. Honduras.* While stronger attribution rules may be necessary to respond to new cyber

[6] Johan Sigholm, 'Non-state actors in cyberspace operations', *Journal of Military Studies* 4, 2013, pp. 1-37, p. 23.
[7] Sigholm,'Non-state actors'.

threats, we argue that the *lex specialis* of human rights responsibility is ultimately unlikely to become the law of cybersecurity responsibility because the international community lacks consensus about enforcing cybersecurity law.

2 Why Do States Break International Law?

To have an effective system of international law—one in which law induces states to behave differently than they would in the absence of law—we must understand why states (do not) comply with international law. Three competing perspectives provide insight: the enforcement, managerial, and flexibility perspectives. These perspectives make different assumptions about how states behave, which yield different arguments about how international law should be designed to promote cooperation.

2.1 Enforcement Perspective

Scholars who adopt an enforcement perspective usually assume that states are rational actors. This assumption requires that leaders have preferences over the outcomes that can result from their choices; and that leaders act instrumentally to try to achieve their preferences, given their beliefs about how other states will act. While political leaders may feel a moral desire to follow international law, they ultimately behave in a way that best protects the interests of their state, regardless of what international law requires. As Jack Goldsmith and Eric Posner argue: 'States do not act in accordance with a rule that they feel obliged to follow; they act because it is in their interest to do so.'[8] Any policy decision is therefore based on a careful calculation of the costs and benefits of possible alternatives, and even if 'citizens and leaders have a preference for international law compliance, preferences for this good must be compared to preferences for other goods.'[9]

[8] Jack L. Goldsmith and Eric A. Posner, *The limits of international law* (Oxford: Oxford University Press, 2005), p. 39.
[9] Goldsmith and Posner, *The limits*, p. 9.

The enforcement perspective assumes that breaking international law often provides leaders a short-term benefit. For example, a leader facing strong domestic political opposition may benefit politically from violating human rights treaties and suppressing his political opponents; a leader fighting a war may be tempted to use prohibited means, like chemical weapons, to gain a military advantage; or a leader with a weak economy may want to bolster it by breaking trade law and unilaterally limiting foreign competition. If international law requires states to do what they would not otherwise do in the absence of the law, then breaking international law can provide states with tangible benefits.

Leaders must balance such temptations against the expected cost of breaking the rules. Although the international system lacks a centralized body to enforce international law by punishing states that break it, many decentralized forms of punishment exist. By 'punishment', we mean any response to a legal violation by states (either individually or collectively) that raises the cost of breaking international law. Possible punishments include legal and political outcomes. If a state has accepted jurisdiction of an international judicial body, a legal breach may lead to formal dispute settlement at a venue like the International Court of Justice or the World Trade Organization. Alternatively, governments may face domestic accountability from citizens who favor compliance. At the international level, a state may face retaliation or damage to its reputation.[10]

The expected cost of punishment depends on the magnitude and likelihood of punishment. Punishments vary greatly in terms of magnitude; for example, economic sanctions and military invasion are much costlier than negative publicity. Thus, raising the magnitude of punishment will raise the cost of non-compliance. However, high-magnitude punishments are not always likely: military intervention is a costly punishment, but if the probability it is used is close to zero, a leader may still find non-compliance optimal. The likelihood of punishment can be affected by many

[10] Andrew T. Guzman, *How international law works* (Oxford: Oxford University Press, 2008).

different factors, including likelihood of detection and the cost of punishing the violator state. All else equal, more powerful states can usually better withstand punishment than less powerful states.

The enforcement perspective suggests that if states wish to bolster the effectiveness of international law, they should write rules and design institutions that increase the likelihood and magnitude of punishment for legal violations. Scholars who adhere to the enforcement perspective would probably point to the Estonian cyberattacks case as evidence of international law's weakness: despite a widespread belief that Russia broke international law, Russia faced no tangible punishment. Moreover, Estonia had few options for punishing Russia. It could not establish jurisdiction of an international court to hear its case, and it could not appeal to the UN Security Council where Russia holds veto power. Instead, Estonia was reliant on NATO—an institution of power politics—to pressure Russia. Additionally, the international community's failure to punish Russia in 2007 appears to have encouraged Russia to commit further attacks.[11] Overall, the enforcement perspective suggests that disconnects between legal breaches and punishments may reduce compliance with international law.

2.2 Managerial Perspective

Scholars who adhere to the managerial perspective believe that the international system is fundamentally characterized by order.[12] Louis Henkin succinctly articulated the managerial perspective:

[11] These include cyber operations during conflicts with Georgia (2008) and Ukraine (2014). See Schmitt, *Tallinn Manual,* p. 376.
[12] See Abram Chayes and Antonia Handler Chayes, 'On compliance', *International Organization* 47, 1993, pp. 175-205.

> [T]he daily, sober loyalty of nations to the law and their obligations is hardly noted. It is probably the case that *almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time*.[13]

The managerial perspective thus begins with the observation that states usually comply with international law.

This perspective puts forward three arguments about why states sometimes break the rules. First, states may have principled disagreements about what the law requires. For example, in the *North Sea* dispute, Denmark and the Netherlands believed that Germany was legally required to use the equidistance method during negotiations over maritime delimitations. In contrast, Germany believed that it was not required to use this method, in part because it believed this rule was fundamentally unfair. A managerial scholar would hold up such a case as an example of principled disagreement about the meaning of law. Neither side opportunistically broke a clear, well-defined rule. Rather, each side made a principled legal argument. Managerial scholars might also argue that states faced significant ambiguity about the details of Estonia's 2007 cyberattack and the legal obligations involved, such that Russia should not be responsible. International law does not have any treaties that specifically address cyberattacks; rather, NATO had to convene a team of experts to clarify the relevant rules. If law experts themselves were uncertain in 2007 about what international law required, how could Russia know any better?

Second, states may sometimes break international law because they lack the capacity to fully comply with the rules. Capacity is likely to be a bigger issue for states that are not economically developed or with weak government institutions. For example, while Indian Prime Minister Narenda Modi said in 2017 it would be a 'morally criminal act' for states to ignore the growing threat of climate change, India's government will find it extremely costly, both

[13] Louis Henkin, *How nations behave* (New York: Columbia University Press, 1979), p. 47. Emphasis in original.

economically and politically, to comply with an environmental agreement that slows industrialization and economic growth.[14] Similarly, governments without effective bureaucracies may lack the capacity to force businesses and consumers to adopt pollution-reducing technologies. A genuine desire to comply may not ensure compliance, particularly when international law constrains private actors. Managerial scholars might also argue that Russia lacked capacity to control its 'hacktivists', so it cannot be responsible for the cyberattack.

Third, states may not comply because they have not had enough time to change their behavior. For example, the WTO is based on rules that were crafted in the late 1940s by a few relatively rich states. As more states joined the trade regime, its members became more diverse, creating challenges for trade cooperation. When China joined in 2001, it had to negotiate a special agreement under which it promised to progressively adopt economic reforms so that its economy would more closely resemble a market economy. Many of China's trade conflicts stem from the pace of Chinese economic reforms. For example, the EU and America often argue that China does not adequately protect intellectual property rights, harming foreign businesses. Yet intellectual property rights have expanded dramatically since 2001 and are likely to grow stronger as Chinese companies develop new technology.[15] Some scholars defend China by arguing that it has not had sufficient time to reform its domestic economic and legal system.[16]

Managerial scholars often argue that international law and institutions should be used to manage compliance by persuading states to comply, rather than punishing them for breaking international law. While courts can reduce ambiguity about legal obligations, adversarial lawsuits and strict rules about state responsibility cannot solve the other challenges of compliance. Harold

[14] See Ben Westcott, 'Reluctant signatory India takes moral high-ground on Paris climate deal', *CNN*, 2 June 2017.
[15] Natalie P. Stoianoff, 'The influence of the WTO over China's intellectual property regime', *Sydney Law Review* 34, 2012, pp. 65-89.
[16] See Xuan-Thao Nguyen, 'The China we hardly know: revealing the New China's intellectual property regime', *Saint Louis University Law Journal* 55, 2011, pp. 773-810.

Hongju Koh argues that 'nations obey international rules not because they are threatened with sanctions, but because they are persuaded to comply.'[17] The managerialist perspective therefore suggests that the international system should help states build capacity and internalize international norms, rather than punish violations.

2.3 Flexibility Perspective

Political scientists originally developed the flexibility perspective to understand the design and operation of international trade law.[18] Like the enforcement perspective, the flexibility perspective emphasizes punishment in inducing states to comply with international law. Yet just as the managerial perspective believes that states often have legitimate reasons for breaking the rules, so too does the flexibility perspective emphasize that states should sometimes be allowed to break their commitments in response to extreme economic or political pressure. International law must therefore be designed in a way that can survive periodic breaches without complete collapse.

The flexibility perspective begins with the assumption that economic and political pressure on governments to break international law can change unexpectedly over time.[19] States will usually find it beneficial to comply with their legal commitments, but unexpected events can tempt states to break international law. For example, after the 2015 terrorist attacks in Paris, France declared a state of emergency and temporarily limited human rights by reducing judicial oversight of police activities. The flexibility perspective assumes that sometimes unexpected events—like economic recessions or terrorist attacks—will make compliance extremely costly.

The flexibility perspective also assumes that states can select into and out of legal commitments over time. As emphasized by the managerial perspective, states would not make legal commitments if they did not believe that these commitments would be followed most of the

[17] Harold Hongju Koh, 'Why do nations obey international law?' *The Yale Law Journal* 106, 1997, pp. 2599-2659, p. 2601.
[18] See B. Peter Rosendorff, 'Stability and rigidity: politics and the design of the WTO's dispute resolution procedure', *American Political Science Review* 99, 2005, pp. 389–400.
[19] See (---).

time. Yet states often exit from international treaties when they can no longer afford to comply with their commitments.[20] Similarly, many states have chosen to renounce the jurisdiction of international courts when they disagree with important court rulings or are unable to comply with them. An optimal legal system is therefore one in which states join cooperative agreements, comply with their commitments, and do not exit their agreements during severe economic or political crises.

The flexibility perspective argues that laws should be designed to allow states to sometimes break commitments without facing severe punishment. Stronger punishments make it costlier in expectation for states to join an agreement: states know they may sometimes face unexpected crises. If every legal breach triggers an extreme punishment, states may simply refuse to join cooperative agreements. Alternatively, they may join, but then exit the moment compliance becomes costly. Strong punishments can thus make treaties unstable over time.

The flexibility perspective proposes that international law include escape clauses, which allow states to temporarily break their legal commitments without facing severe punishments when facing unexpected and severe economic and political pressure. While Estonia's decision to move the Bronze Soldier and Soviet graves did not legally excuse or justify a cyberattack, it does explain why Russians were angry with Estonia. From Russia's perspective, Estonia's actions triggered political pressure on the Russian government to respond. Similarly, investment law allows states to violate property rights in response to economic emergencies, and many human rights agreements allow states to suspend some civil liberties during temporary crises.[21] Escape clauses have three primary benefits: they make states more likely to join cooperative agreements in

[20] Laurence R. Helfer, 'Exiting treaties', *Virginia Law Review* 91, 2005, pp. 1579-1648.
[21] Emilie M. Hafner-Burton, Laurence R. Helfer, and Christopher J. Fariss, 'Emergency and escape: explaining derogations from human rights treaties', *International Organization* 65, 2011, pp. 673–707.

the first place;[22] they allow states to make deeper commitments to cooperation, such as pledging to remove more trade barriers or protect more human rights;[23] and they survive longer.[24] All of these benefits result from allowing states to sometimes break international law without suffering negative consequences.

3 Understanding General Rules of Attribution

The international law of state responsibility developed from disputes over the treatment of individuals and businesses in foreign states in the nineteenth and early twentieth centuries.[25] Over time, the International Law Commission (ILC) codified these rules, creating general rules of state responsibility that are written in the Articles on State Responsibility (2001). The UN General Assembly expressed formal support for the ILC Articles. While the Articles were not transformed into treaty law, they have been invoked by judges, scholars, and states as customary international law, one of the main sources of international law.[26] We therefore use the ILC Articles for our discussion on general rules, noting debates over these rules where appropriate.

The ILC Articles identify three aspects of state responsibility: attribution, wrongfulness, and consequences.[27] Attribution rules refer to when a particular act or omission is considered conduct of a state.[28] Wrongfulness determines whether a breach actually violates international law, or if a circumstance, such as necessity or duress, might preclude wrongfulness. Finally, the idea of consequences refers to the types of punishments, or costs, that states endure for committing

[22] Jeffrey Kucik and Eric Reinhardt, 'Does flexibility promote cooperation? An application to the global trade regime', *International Organization* 62, 2008, pp. 477–505.
[23] See (---).
[24] Rosendorff, 'Stability and rigidity'.
[25] Alan Nissel, 'The duality of state responsibility', *Columbia Human Rights Law Review* 44, 2013, pp. 793-858.
[26] See (---).
[27] For a more detailed introduction to these rules, See Malcolm N. Shaw, *International law* (Cambridge: Cambridge University Press, 2017), p. 589—639.
[28] We use the term 'conduct' as the ILC rules cover both acts and omissions.

wrongful breaches of the law. The strength of any of these aspects can vary across issue areas; for example, the *lex specialis* of trade law recognizes many circumstances that preclude wrongfulness of violating trade agreements and some human rights treaties allow for derogation – temporary suspension of rights guaranteed within the treaty. In terms of consequences, some human rights courts impose higher costs for violating the law than trade courts.[29] For the purposes of this paper, however, we choose to focus on attribution rules, as we believe these represent the most important area be strengthened in order to adequately counter cyber threats.

3.1 Attribution Rules for State Actors

Attribution rules determine whether conduct can be attributed to a state. In particular, they ask who specifically has committed the conduct, and whether the state had capacity to control that actor. By emphasizing capacity, they usually reflect the managerial perspective on compliance. Only sometimes—when states are held responsible for non-state actors under their overall control—do they reflect the enforcement perspective.

Under international law, a state is responsible for the conduct of all its bodies.[30] International law does not distinguish between conduct of national, regional, or local governments. A state is responsible for all of its bodies, meaning that states with federal governments, like Mexico and the US, often face special challenges when complying with international law. Even if the national government cannot order a regional or local government to behave in a particular way, the state is still responsible for its regional and local governments. Similarly, even if an executive

[29] On the use of escape clauses in trade law, see Krzysztof J. Pelc, 'Seeking escape: the use of escape clauses in international trade agreements', *International Studies Quarterly* 53, 2009, pp. 349-368. On the specific exceptions to human rights treaties (derogations), see Hafner-Burton, Helfer, and Fariss, 'Emergency and escape.' On low levels of punishment in trade law, see Rachel Brewster, 'The remedy gap: institutional design, retaliation, and trade law enforcement', *George Washington Law Review* 80, 2011, pp. 102-156. On consequences in human rights courts, see (---).

[30] International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' ('ILC Commentary') UN Document A/56/10, 2001. Article 4, para. 1.

cannot compel a legislature or court to behave in a certain way, the state is still responsible for all of its branches of government.

While it is relatively straightforward to determine attribution for the conduct of government bodies, it is more difficult to assess the conduct of individuals with state authority, like government officials, because they are sometimes state agents, and other times private individuals, acting independently of their employer. International law deals with these dual lives by examining the authority and capacity of agents. Broadly speaking, authority usually refers to the legally allowable conduct of an individual. For example, most states give police officers authority to arrest and detain individuals who are suspected of committing crimes. However, they usually do not give police officers authority to torture suspects. Such conduct is referred to as *ultra vires* ('beyond the powers'): it lies outside of the authority given by the state to its agent. In contrast, capacity usually refers to how others might interpret the agent's conduct, given the overall context. The ILC argued that even if a government official acts outside of his legal authority, the state is responsible if he acts in his capacity as a government official.

These rules reflect managerial concerns about compliance. Although attribution rules are strict for government bodies, they are more relaxed for government officials. These rules implicitly assume that states can mostly control their employees. However, they also recognize that states do not have absolute control over their employees, meaning that a state is not responsible for its agents' private acts.

3.2 Attribution Rules for Non-State Actors

States can also be responsible for breaches of international law committed by non-state actors. The ILC Articles say that 'The conduct of a person … shall be considered an act of a State … if the person … is in fact acting on the instructions of, or under the direction or control of, that State.'[31]

[31] ILC Commentary, Article 8.

In practice, there is often disagreement about how to implement this standard. International courts have articulated two approaches: the effective and overall control standards.

The ICJ created the effective control standard in the *Nicaragua* case (1986), when it ruled on US military involvement in Nicaragua in the 1980s. The US government provided support to rebels challenging Nicaragua's Sandinista government, which the US perceived as a Communist threat. In its ruling, the ICJ distinguished between three types of actors: US government personnel, who primarily worked for the US military and Central Intelligence Agency; 'Unilaterally Controlled Latino Assets' (UCLAs), who were 'persons of the nationality of unidentified Latin American countries, paid by, and acting on the direct instructions of, United States … personnel';[32] and Nicaraguan rebels, called the *contras*.

The ICJ argued that the US was responsible for the conduct of the UCLAs because of its extensive involvement in planning and supporting UCLA acts.[33] However, the ICJ found that the US played a more limited role in supporting the *contras,* which Nicaragua accused of numerous crimes. The US provided funding, intelligence, supplies, and training for the *contras*. But the Court did not believe that the *contras'* operations 'reflected strategy and tactics wholly devised by the United States.'[34] According to the ICJ, the US could only be responsible for the conduct of the *contras* if it had 'effective control' over them.[35] Nicaragua could not prove that the US directed the *contras* to commit the alleged crimes, so the US was not responsible for their conduct.

The International Criminal Tribunal for Yugoslavia (ICTY) proposed an alternative standard in the *Tadić* case: the overall control standard. The ICTY argued that just as states were responsible for *ultra vires* acts of their officials, so too are they responsible for the conduct of military and

[32] ICJ, *Nicaragua v. United States* (1986), para. 75.
[33] *Nicaragua*, para. 86.
[34] *Nicaragua*, para. 106.
[35] *Nicaragua*, para. 115.

paramilitary groups under their overall control, regardless of whether these groups are following the explicit directions or instructions from the state. It argued that attribution requires:

> that the State wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity … However, it is not necessary that … the State should also issue … instructions for the commission of specific acts contrary to international law.[36]

The overall control standard thus requires less than the effective control standard to establish that a state is responsible for the behavior of non-state actors.

The ICJ revisited its *Nicaragua* ruling in 2007 when it heard a lawsuit about the Srebrenica genocide. Rather than adopt the overall control standard, the ICJ reaffirmed its *Nicaragua* ruling, arguing that:

> the 'overall control' test … broaden[s] State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct … the 'overall control' test is unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility.[37]

The effective control standard is a relatively weak attribution rule because it allows states to avoid responsibility for the conduct of non-state actors. By emphasizing managerial concerns about the capacity of states to control non-state actors, the effective control standard diminishes deterrence via punishments for legal violations. The ICJ's adherence to the effective control standard suggests that it views managerial concerns as more salient than enforcement. In contrast, the overall control standard is a relatively strong attribution rule that privileges enforcement over managerial concerns.

---

[36] ICTY, *Prosecutor v. Tadić* (1999), para. 131.
[37] ICJ, *Bosnia and Herzegovina v. Serbia and Montenegro* (2007), para. 406.

Finally, even if a state has no control over non-state actors, it can become responsible for their behavior if the state 'acknowledges and adopts the conduct in question as its own.'[38] As the ILC noted, this requires that a state offer more than 'mere support or endorsement' of the conduct.[39] Such situations are rare, but the ICJ held Iran responsible for legal violations after its officials supported the 1979 attacks on American embassies and consulates in Iran.[40]

Attribution rules in international law appear to mostly match the concerns of the managerial perspective: when states have less capacity to control officials and non-state actors, they are less responsible. This ensures that states are not punished for outcomes that they cannot control.[41] In the Estonian cyberattacks, Russia claimed that it could not control the 'hacktivists' who attacked business and government websites. The NATO experts argued there was insufficient evidence for attribution because 'there is no definitive evidence that the hacktivists involved in the cyber operations against Estonia in 2007 operated pursuant to instructions from any State, nor did any State endorse and adopt the conduct.'[42] Accordingly, they found that Russia was not responsible for the cyberattack.

While attribution rules are designed with capacity in mind, they may also allow states to maintain flexibility. Specifically, by creating incentives for states to outsource legal violations to non-state actors, attribution rules also grant states the flexibility to violate international law during tough times without facing legal consequences. Thus, attribution rules largely reflect managerial concerns, and to some extent create flexibility, but overall do not prioritize enforcement.

---

[38] ILC Commentary, Article 11.
[39] ILC Commentary, p. 53.
[40] ICJ, *United States v. Iran* (1980), para. 71 and 74.
[41] The one exception to this conclusion lies in those courts, like the ICTY, that support the overall control standard. When this standard is used, enforcement is more likely, because states are unable to evade responsibility by claiming the behavior was out of their control, or worse, to outsource legal violations to non-state actors. See ICTY, *Tadić*, para. 117.
[42] Schmitt, *Tallinn Manual,* p. 382.

4 Towards *Lex Specialis:* Attribution Rules in the Inter-American Court of Human Rights

Attribution rules under the *lex generalis* on state responsibility create multiple disconnects between legal breaches and punishment, which privilege the concerns of the managerial perspectives on compliance. However, international law can be designed differently when states want to prioritize enforcement. For example, states that have recently transitioned from autocracy to democracy might want strong state responsibility rules for human rights to deter violations and prevent a backslide to autocracy.[43] What might these rules look like? In a regime designed around enforcement, states must create stronger rules around attribution.

To illustrate how states can craft stronger attribution rules, we consider the IACHR, a Latin American human rights court. Most IACHR members joined the court after transitioning from military dictatorship to democracy in the 1980s. The American Convention on Human Rights and the IACHR have created strong state responsibility rules to prevent future human rights violations, beginning with strict rules on attribution that prevent outsourcing of violations to non-state actors.

As with the *lex generalis* on state responsibility, IACHR members are responsible for all government bodies and for agents acting in their official authority or capacity. This includes *ultra vires* acts of government officials using their official capacity, as established in *Velásquez Rodríguez v. Honduras.* Most IACHR violations are committed by government agents, including military and police officers.[44] Thus, states usually cannot avoid responsibility based on attribution.

For non-state actors, the IACHR often attributes conduct of private individuals to states, even if those individuals are not controlled by the state. Namely, the IACHR's 'complicity standard'

---

[43] See, e.g., Emilie M. Hafner-Burton, Edward D. Mansfield, and Jon C.W. Pevehouse, 'Human rights institutions, sovereignty costs and democratization', *British Journal of Political Science* 45, 2015, pp. 1-27; Andrew Moravcsik, 'The origins of human rights regimes: democratic delegation in postwar Europe', *International Organization* 54, 2000, pp. 217-252; and Simon Zschirnt and Mark Menaldo, 'International insurance? Democratic consolidation and support for international human rights regimes', *International Journal of Transitional Justice* 8, 2014, pp. 452-475.
[44] See (---).

holds states responsible if they provide 'a knowing and causal contribution to the commission of a conduct by a non-state actor,' which entails any form of aid or assistance.[45] In *Mapiripán Massacre v. Colombia*, the IACHR wrote*:*

> States … have … obligations … to ensure the effectiveness of the rights … under any circumstances and regarding all persons. The effect of these obligations … is … reflected in the positive obligation of the State to take such steps as may be necessary to ensure effective protection of human rights in relations amongst individuals. The State may be found responsible for acts by private individuals in cases in which, through actions or omissions by its agents when they are in the position of guarantors, the State does not fulfill these … obligations.[46]

Thus, if a state assists or fails to prevent a violation by a private individual, the state can be responsible for that violation. In *Mapiripán Massacre v. Colombia*, the Court found that Columbia was responsible for a massacre by paramilitary groups because 'the massacre could not have been prepared and carried out without the collaboration, acquiescence, and tolerance … of the Armed Forces.'[47]

Similarly, the American Convention requires its members to 'ensure the free and full exercise' of rights, which the state can violate by failing to investigate alleged criminal acts. In *Kawas Fernández v. Honduras*, the IACHR examined a murder committed by private individuals in Honduras. Even though Honduran state employees did not commit the murder, they failed to adequately investigate it. The IACHR argued that this failure meant that the murderers were 'assisted by public authorities.'[48] This assistance, in turn, meant that Honduras was responsible for violating the Convention's right to life.

---

[45] Vladyslav Lanovoy, 'The use of force by non-state actors and the limits of attribution of conduct', *European Journal of International Law* 28, 2017, pp. 563-585, p. 585.
[46] IACHR, *Mapiripán Massacre v. Colombia* (2005), para. 111.
[47] IACHR, *Mapiripán Massacre*, at 120.
[48] IACHR, *Kawas Fernández,* para. 78.

The complicity standard deters human rights violations by encouraging states to domestically prevent and punish violations. By this standard, states are responsible for violations of the American Convention even when their agents do not commit the actions, and even if there is no active relationship between government agents and the perpetrators. Thus, states cannot evade responsibility by 'outsourcing' violations to non-state actors. Moreover, they cannot turn a blind eye to non-state actors who commit violations, as failing to investigate alleged crimes can incur responsibility under international law.

5 Conclusion: *Lex Specialis* for Cyberattacks?

We began by examining the 2007 cyberattacks against Estonia and the case of *Kawas Fernández v. Honduras* at the Inter-American Court of Human Rights. Both examples involved legal violations that were committed by individuals. However, Honduras was found responsible for legal violations under the *lex specialis* of human rights at the Inter-American Court, while Russia was not found responsible for the cyberattack under the *lex generalis,* which applied to hacking.

The development and jurisprudence of the Inter-American Court of Human Rights illustrates how states can develop rules that place less emphasis on managerial concerns when they have a common goal that is served by enforcement. The IACHR's jurisprudence prevents states from outsourcing violations to non-state actors because even these acts can be attributed to the state if, for example, the state fails to investigate them. States in the Inter-American system were able to cooperate and establish strict rules because they were committed to preventing future human rights violations. Could such logic extend to the realm of hacking? In other words, might states develop a *lex specialis* for cyberattacks that prioritizes enforcement?[49]

[49] We note here that while Rex Hughes' proposed treaty for cyberspace addresses many other issues, including *jus ad bellum* questions like military necessity and *jus in bello* questions like discrimination, he does not explicitly address how to hold states responsible under international law for violations of such a treaty, particularly if the violations are committed by non-state actors. See Hughes, 'A treaty for cyberspace'.

If states wanted to prevent future cyberattacks, they would need to start by developing a stronger attribution rule. The general rules might incentivize states to outsource legal violations to individual hacktivists, over whom they do not have effective control. For example, Scott J. Shackelford and Richard B. Andres argued:

> Given the secretive nature of cyber conflict, States may incite civilian groups within their own borders to commit cyber attacks and then hide behind a (however sheer) veil of plausible deniability, thus escaping accountability.[50]

To prevent this evasion of responsibility, a *lex specialis* for cyberattacks would need to recognize the potential role of states in facilitating cyberattacks. The Inter-American Court was able to establish the complicity standard because it held that the mere failure to investigate a murder incurred responsibility for the original legal violation. If a *lex specialis* for cyberattacks could establish stricter means of holding states accountable – for example, by incurring responsibility for failure to prevent cyberattacks – states might be more inclined to crack down on the hackers. Under such a complicity standard, if Estonia could show that Russia knew about the actions of the 'hacktivists' and failed to prevent them, Russia could be held responsible for the cyberattack. Alternatively, if Russia failed to investigate the cyberattack after the fact to determine who the 'hacktivists' were, Russia could be responsible for the cyberattack under a complicity standard, much like Honduras was responsible for the murder of Kawas Fernández, even though her death was ultimately carried out by private individuals unaffiliated with the state.

Numerous legal scholars have proposed alternative rules that they believe states should adopt for regulating cyberattacks to strengthen enforcement. However, most of these have focused on what acts would count as cyberattacks: states must agree on a basic definition of what conduct counts as a cyberattack before addressing more complicated issues such as attribution. For

[50] Scott J. Shackelford and Richard B. Andres, 'State responsibility for cyber attacks: competing standards for a growing problem', *Georgetown Journal of International Law* 42, 2011, pp. 971-1015. p. 975.

example, Rebecca Croontof proposes defining a class of 'cybertorts' to distinguish these acts from other forms of cyber warfare.[51] Additionally, Oona Hathaway and several co-authors specifically define 'cyber-crime' as committed by non-state actors, while cyberattacks and cyber-warfare can be committed by the state.[52] However, it is important to remember that none of these proposed rules are actually part of international law. States, not law professors, make international law. Moreover, even if these proposals were adopted, they might further muddy the waters around attribution of cyberattacks by non-state actors by explicitly defining such attacks as a separate class of legal violations. This might even encourage states to outsource cyberattacks to non-state actors because attacks by non-state actors could be classified as a separate type of violation that might incur fewer consequences. Thus, even existing proposals do not do enough, in our view, to adequately address cyber threats because they do not explicitly address gaps in enforcement resulting from weak attribution rules.

Why have states refused to strengthen attribution rules for cyberattacks? We believe that the explanation is quite simple: states do not want to prevent all cyberattacks. They privilege flexibility at the expense of enforcement. While NATO members do not want Russia to attack Estonia, they also want to preserve their own flexibility to commit attacks against their adversaries.[53] For example, the US has publicly been highly critical of states like China, North Korea, and Russia for allegedly conducting cyberattacks within the US to access business and military secrets. Yet the US is also widely believed to have conducted the first ever cyberattack, which occurred in 1982 when a Soviet pipeline in Siberia exploded based on malicious computer

[51] Rebecca Crootof, 'International cybertorts: expanding state accountability in cyberspace', *Cornell Law Review* 103, 2018, pp. 565-644.
[52] Oona Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, 'The law of cyber-attack', *California Law Review* 100, 2012, pp. 817-886.
[53] Some states, such as France, may also be concerned about cooperating too deeply on issues of cyber security, given the nature of the weapons. See Alice Pannier and Olivier Schmitt, 'To fight another day: France between the fight against terrorism and future warfare', *International Affairs* 95, 2019, pp. 897-916.

code that the CIA had planted in Canadian software.[54] Similarly, a computer glitch revealed to the world in 2010 the existence of Stuxnet, a sophisticated computer program that could 'worm' into computer operating systems and disrupt industrial control systems. Years of investigative reporting led to revelations that Stuxnet was a joint creation of Israel and the US, which had been using the program since 2006 to hinder Iran's nuclear centrifuges.[55] While major programs like Stuxnet may presently be too costly for non-state actors to create on their own, as the cyberattack on Estonia shows, non-state actors may still launch costly attacks with less sophisticated programs.[56]

As such, temptations to commit cyberattacks may simply be too large for effective cooperation on this issue. Any apparent opposition to cyberattacks is therefore likely to be mere rhetoric, at best, and hypocrisy, at worst: states want to retain the ability to use cyberweapons, even if they would rather not have the weapons used on themselves. In the case of cybersecurity, the general law on state responsibility will apply unless and until the international community decides that preventing all attacks is more important than preserving its own ability to launch them.

[54] See 'Cyberwar: war in the fifth domain', *The Economist*, 3 July 2010.
[55] See David E. Sanger, 'Obama order sped up wave of cyberattacks against Iran', *New York Times*, 1 June 2012.
[56] Warren Chin, 'Technology, war and the state: past, present and future', *International Affairs* 95, 2019, pp. 765-783.