Chicago Journal of International Law

Volume 10 | Number 2 Article 14

1-1-2010

A State's Duty to Prevent and Respond to Cyberterrorist Acts

Christopher E. Lentz

A State's Duty to Prevent and Respond to Cyberterrorist Acts

Christopher E. Lentz*

Cyberterrorism combines two of the most prominent developments of the last twenty years: the increasing reliance on the internet's infrastructure, and the threat of international terrorism committed by non-state actors. Although multilateral treaties aim to shore up some aspects of cybercrime, and the Security Council has taken steps towards preventing terrorist acts, international law appears to lack a cohesive approach for dealing with situations where cyberspace and terrorism overlap. This Comment proposes one such approach for tackling the emergent problem of cyberterrorism.

International law has yet to articulate a satisfactory prohibition on, or definition of, "terrorism." Instead, international agreements ban specific acts as inherently terrorist, although none of these bans clearly encompass cyberacts. While these agreements can be dispositive, the Security Council revealed its willingness after September 11 to identify, on an ad hoc basis, "terrorist acts." The Security Council then wrote Resolution 1373 in a way that created an international duty that commands all states to prevent and respond to terrorist acts. This Resolution should be interpreted to recognize a similar duty on all states to prevent and respond to cyberterrorist acts, whenever they are identified as such. Recognizing this duty will probably lead to negligible changes in states' preventative acts, but it should establish a fundamental and reasonable responsibility on states to cooperate in response to the inevitable cyberterrorist act.

I. INTRODUCTION

Cyberattacks are at the forefront of international conflict. Estonia learned this in 2007 when its "paperless government" faced an extended cyberattack after upsetting Russia.[1] Estonia initially claimed that Russia had directed these

* BA 2003, Tufts University; JD 2009, The University of Chicago Law School.

1 See *The Cyber Raiders Hitting Estonia*, BBC News (May 17, 2007), online at http://news.bbc.co.uk/1/hi/world/europe/6665195.stm (visited Nov 21, 2009) (reporting that Estonia's defence ministry compared these cyberattacks to "terrorist activities").

attacks but later seemed to withdraw this claim,[2] possibly because of the inherent difficulty of demonstrating the attacks were state, or state-sponsored, action. Instead, Estonia published a list of IP addresses, mostly located in Russian territory, from where it believed the cyberattacks emanated.[3] The following year, it appeared this pattern started to repeat itself when Georgia became the newest target of alleged Russian hackers responding to actual fighting between the two states.[4]

These cyberattacks against Estonia and Georgia appear to confirm that individuals are capable of utilizing the internet to harass states. What will happen when cyberharassment inevitably grows into cyberterrorism on a catastrophic scale? The victim states will surely strive to identify their attackers, and might calibrate their responses accordingly. But this identification will almost certainly require the cooperation of other states, including the state from where the attack originated. Such cooperation, though, may not be forthcoming merely as a matter of compassion. Instead, states might only acquiesce in providing assistance if obligated through an international law duty.[5]

But international law currently recognizes no such duty as incumbent on all states. Despite the wave of cyberterrorism that seems poised to threaten world security, international law has yet to solidify an appropriate response

---

2 Compare *Estonia Hit By 'Moscow Cyber War'*, BBC News (May 17, 2007), online at http://news.bbc.co.uk/1/hi/world/europe/6665145.stm (visited Nov 21, 2009) ("Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.") with BBC News, *The Cyber Raiders Hitting Estonia* (cited in note 1) ("[T]he government in Tallinn has not blamed the Russian authorities directly for the attacks.").

3 BBC News, *The Cyber Raiders Hitting Estonia* (cited in note 1) (stating that these IP addresses included some "in the Russian government and presidential administration").

4 Consider Neil Arun, *Caucasus Foes Fight Cyber War*, BBC News (Aug 14, 2008), online at http://news.bbc.co.uk/1/hi/world/europe/7559850.stm (visited Nov 21, 2009) (reporting, ominously, the opinion of internet security experts who claimed "it was inevitable that . . . [such a conflict] should spill into cyberspace").

5 States do not always observe their international law duties, of course. But recognizing these duties is a prerequisite for recognizing when a state has breached them. See International Law Commission, *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, Art 12, [2001] Vol II (Part Two) YB Intl L Commn 26, UN Doc A/56/10 ("There is a breach of an international obligation by a State when an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character.") This, in turn, helps to determine when an injured state may lawfully employ countermeasures to force the breaching state to fulfill its obligations. See id at Art 49(1) (offering the limits of countermeasures). This Comment focuses on international law, not on how states will respond to this law. The realist critique of international law may be an important one, but responding to it is not within this Comment's purview.

mechanism.[6] This Comment aims to advance one possible means to help states collectively withstand the ominous threat of cyberterrorist attacks.

Sections II.A. and II.B address international law's inability to formulate a workable prohibition on terrorism, leading to a focus on terrorist acts. Section II.C demonstrates that especially egregious acts can be defined as "terrorist" after they occur, and it introduces Security Council Resolution 1373, which creates binding duties upon all states to prevent and respond to "terrorist acts." Section III looks at cyberterrorist acts from a victim state's perspective, showing that state cooperation will be essential for identifying the perpetrators. It also points out that attributing cyberterrorist acts to other states will be practically impossible, thereby calling for a solution that obliges states to play a role in the realm of cyberterrorism. Section IV proposes interpreting Resolution 1373 to recognize an international law duty for states to prevent or respond to any cyberterrorist act. Because of issues defining cyberacts as "terrorist," the forward-looking duty to prevent cyberterrorist acts will have minimal practical effect. But there will be no definitional dilemma for the backward-looking duty to respond. When triggered, this latter duty entails reasonable obligations to cooperate in criminal investigations and to arrest, and prosecute or extradite, an alleged cyberterrorist actor.

II. INTERNATIONAL LAW'S FOCUS ON TERRORIST ACTS

Questions regarding cyberterrorism might prove relatively easy to resolve if international law were more settled regarding traditional forms of terrorism. International law, however, has not grappled successfully with terrorism. Section II.A concludes that terrorism has yet to be proscribed by a universally agreed-upon *jus cogens* norm, so that there is no such norm that could be expanded to cover novel forms of terrorism. Section II.B observes that there is not even agreement on how to define "terrorism," which has necessitated an ad hoc system that bans certain types of acts considered to be inherently terroristic. The focus on "terrorist acts" is considered further in Section II.C, which looks at the international response to the September 11 attacks in order to identify international law duties and corollaries to cyberterrorist acts.

---

6 See, for example, Jon P. Jurich, *Development: Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations*, 9 Chi J Intl L 275, 295 (2008) (concluding that "existing law seems unable to cope with the potential harms presented by [offensive or defensive cyberactions]").

A. Problems Concluding That *Jus Cogens* Proscribe Terrorism

Jus cogens—sometimes referred to as "peremptory norms"—are absolute rules that affirm the lawful conduct of all states.[7] The Vienna Convention on the Law of Treaties (Vienna Convention) defines them as "a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted."[8] As such, they are considered laws themselves, rather than sources of law. The actual sources of *jus cogens* norms, though, are in dispute. "The source of peremptory norms has been variously attributed to state consent, natural law, necessity, international public order, and the development of constitutional principles."[9] This lack of agreement on *jus cogens*' ethereal origins is largely irrelevant, however, if there is consensus on the substantive content of the norms.

Unfortunately, no such consensus exists. It seems that "[t]he most obvious and best settled rules of *jus cogens* . . . [include] trade in slaves, piracy or genocide," although other areas are not quite as settled.[10] A laundry list of more controversial norms has also been put forth as worthy of *jus cogens* recognition, including "all human rights, all humanitarian norms[,] . . . the duty not to cause transboundary environmental harm, freedom from torture, the duty to assassinate dictators, the right to life of animals, self-determination, the right to development, free trade, [ ] territorial sovereignty [and] the invalidity of treaties that conflicted with" Soviet ideas of transnational law.[11]

Most pertinent here, it is still disputed whether *jus cogens* prohibit terrorism.[12] For example, the American Law Institute listed "offenses recognized by the community of nations as of universal concern" to include "piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and *perhaps* certain

---

7 See Barry E. Carter, Phillip R. Trimble, and Allen S. Weiner, *International Law* 120 (Aspen 5th ed 2007) (observing that they are "so fundamental that they bind all states").

8 Vienna Convention on the Law of Treaties (1969), Art 53, 1155 UN Treaty Ser 331 (continuing that *jus cogens* norms "can be modified only by a subsequent norm of general international law having the same character").

9 Dinah Shelton, *Normative Hierarchy in International Law*, 100 Am J Intl L 291, 302 (2006) (reaching this conclusion after surveying various sources).

10 International Law Commission, *Draft Articles on the Law of Treaties with Commentaries*, [1966] Vol II YB Intl L Commn 187, 248 (revealing that the International Law Commission intentionally excluded examples of *jus cogens* norms in order to prevent the resulting treaty from being interpreted based on its omissions, and to avoid becoming embroiled in an ongoing dispute over adding *jus cogens* norms that are more controversial).

11 Shelton, 100 Am J Intl L at 303 (cited in note 9) (concluding that "the literature has abounded in claims that additional international norms constitute *jus cogens*").

12 This remains true even if there is no dispute over how to identify "terrorism." This issue is addressed, but not resolved, in Section II.B.

acts of terrorism."[13] This equivocation highlights that a *jus cogens* norm falls short of the Vienna Convention's requirement that the norm be "accepted and recognized by the international community of States."

In addition, although many postulate that a prohibition on terrorism exists,[14] numerous states still engage in some form of terrorism.[15] This calls into question whether the proposed prohibition meets the Vienna Convention's additional condition that the norm be one "from which no derogation is permitted." State participation in terrorism further weakens the argument that a universal terrorism prohibition has been established already.[16]

The disagreement over whether *jus cogens* proscribe terrorism, coupled with state practice in support of terrorism, militates against deciding conclusively that such a proscription exists. Thus, this Comment cannot take a generalized ban on terrorism and broaden it to include cyberterrorism. As a result, this Comment operates under the assumption that a *jus cogens* norm prohibiting terrorism has yet to crystallize fully. It looks elsewhere for a state's duty pertaining to cyberterrorism.

B. Problems Defining "Terrorism" Lead to Proscriptions of Terrorist Acts

After *jus cogens*, the next place to look for an international law ban on terrorism is at the global regime created by the United Nations (UN). The UN has succeeded in roundly condemning "terrorism," even before the galvanizing attacks on September 11.[17] Despite these agreements, the UN and the

---

13 Restatement (Third) of Foreign Relations Law § 404 (1987) (emphasis added) (listing when universal jurisdiction exists for a state to define and punish an offense).

14 See, for example, Viktor Mayer-Schonberger and Teree E. Foster, *More Speech, Less Noise: Amplifying Content-based Speech Regulations Through Binding International Law*, 18 BC Intl & Comp L Rev 59, 100–01 (1995) (identifying the prohibition on terrorism as a *jus cogens* norm that is "[l]argely [u]ndisputed").

15 See, for example, Restatement (Third) of Foreign Relations Law at § 404 cmt a (cited in note 13) ("There has been wide condemnation of terrorism, but international agreements to punish it have not, as of 1987, been widely adhered to.").

16 See Christos L. Rozakis, *The Concept of Jus Cogens in the Law of Treaties* 77–80 (North-Holland 1976) (focusing on the Vienna Convention's language "as a whole" and on the drafting history behind Article 53 to conclude that "the existence of contrary practice by a number of States weakens the evidential position of that norm").

17 See, for example, Resolution 1269, UN Security Council, 4053d mtg (Oct 19, 1999), UN Doc S/RES/1269 ¶ 1 ("*condemn*[*ing*] all acts, methods and practices of terrorism as criminal and unjustifiable"); Resolution 49/60, UN General Assembly, 49th Sess (Dec 9, 1994), UN Doc A/RES/49/60 (Feb 17, 1995) ¶ 4 ("*urg*[*ing*] States . . . to take all appropriate measures . . . to eliminate terrorism"); Resolution 2625 (XXV), UN General Assembly, 25th Sess (Oct 24, 1970), UN Doc A/8018 122–23 ("*proclaim*[*ing*]" the principle that "[e]very State has the duty to refrain

international community as a whole have failed to define this elusive concept.[18] Although this failure arises partly from geopolitics, it stems also from the commonly held belief that "one man's terrorist is another man's freedom fighter."[19] This prevents universal agreement on who constitutes a terrorist, thereby precluding agreement on what constitutes terrorism.

Instead of defining "terrorism," the UN has forged agreements that proscribe acts associated with terrorism.[20] To date, thirteen international instruments have taken aim at such acts. These include conventions proscribing aircraft hijackings, aviation sabotage, hostage taking, and the unlawful theft and use of nuclear material.[21] It is worth noting that none of these conventions clearly relates to cyberterrorism.[22]

These thirteen instruments represent the international community's greatest successes in consensus-building against terrorist acts. But they ban only acts associated with terrorism, not terrorism itself. As a result, there is no clear treaty-based proscription of terrorism, much like there is no clear *jus cogens* prohibition of terrorism, which can be elucidated and expanded upon. Only a specific act that is deemed "terrorist" will trigger any international law duty associated with terrorism. This becomes important when considering the duties created by the Security Council after the September 11 attacks.

C. September 11 and Security Council Resolution 1373

On September 11, 2001, terrorists shocked the world by hijacking four commercial airplanes and turning them into oversized missiles. Two planes crashed into the World Trade Center, precipitating its collapse. One plane flew

---

from organizing, instigating, assisting or participating in ... terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts ... involve a threat or use of force").

18 See Restatement (Third) of Foreign Relations Law at § 404 cmt a (cited in note 13) (noting the international community's "inability to agree on a definition of the offense").

19 See, for example, Alison Elizabeth Chase, *Legal Mechanisms of the International Community and the United States Concerning State Sponsorship of Terrorism*, 45 Va J Intl L 41, 93–96 (2004) (recording this belief as one reason why there has been no international agreement defining "terrorism").

20 See id at 95 (making this observation).

21 See Counter-Terrorism Committee Executive Directorate, *International Counter-Terrorism Instruments* (UN Dept Pub Info 2006) 1–3, online at http://www.un.org/terrorism/pdfs/bgnote_legal_instruments.pdf (visited Nov 21, 2009) (discussing the thirteen conventions).

22 The other nine conventions cover in-flight safety, violence at international airports, terrorist activities on ships and on fixed offshore platforms, attacks on high-ranking government officials or diplomats, marking plastic explosives for identification, bombings in public places, financing of terrorism, and acts of nuclear terrorism. See id at 3–5.

into the Pentagon, and passengers grounded the fourth plane on its way to Washington, DC.[23]

Few doubted that this amounted to terrorist action. The very next day, the Security Council passed Resolution 1368, condemning "the horrifying terrorist attacks" and announcing that it "*regard[ed]* such acts, like any act of international terrorism, as a threat to peace and security."[24] Perhaps unsurprisingly, the Security Council simply labeled these actions as "terrorist attacks." It did not bother to support this assertion by pointing to conventions on aircraft hijackings, aviation sabotage, or other potentially related fields.[25] It just labeled them "terrorist attacks," and moved on to more contentious issues. The General Assembly did exactly the same.[26]

This pattern of events permits two conclusions to be drawn that are particularly relevant to this Comment. First, the resolution focused on "*acts* . . . of international terrorism," rather than on undefined terrorism.[27] This further denied a general, expandable prohibition on terrorism, prolonging the need to identify terrorist acts. Second, and of greater significance, is the realization that the Security Council is capable of immediately recognizing the worst terrorist acts as such.[28] Because the Security Council can promptly identify when a state has been the victim of a terrorist act, there need be no debate over definitional issues—at least not in the most extreme examples. It is these "horrifying" cases that this Comment hopes to address.

The Security Council did not limit its response to the September 12 resolution that offered mere recognition and condemnation. It also passed Resolution 1373, which has been "[d]escribed as one of the most strongly worded resolutions in the history of the Security Council."[29] In Resolution 1373,

---

23 See National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* 4–14 (Norton 2004).

24 Resolution 1368, UN Security Council, 4370th mtg (Sept 12, 2001), UN Doc S/RES/1368 ¶ 1.

25 The Security Council cited only one decree. See id, citing Resolution 1269 at ¶ 1 (cited in note 17) ("[C]ondemn[ing] all acts, methods and practices of terrorism as criminal and unjustifiable.").

26 See Resolution 56/1, UN General Assembly, 56th Sess (Sept 12, 2001), UN Doc A/RES/56/1 (Sept 18, 2001) ("*The General Assembly* . . . [*s*]*trongly condemns* the heinous acts of terrorism [the previous day].").

27 Resolution 1368 at ¶1 (cited in note 24) (emphasis added). Consider also Resolution 56/1 at ¶ 1 (cited in note 26) (condemning "the heinous acts of terrorism").

28 Consider Thomas M. Franck, *Recourse to Force: State Action Against Threats and Armed Attacks* 66 (Cambridge 2002) (comparing the Security Council's response after September 11 with its more qualified responses to other attacks, and concluding that "[p]resumably, it is clarity of the facts, the evidence, and the context that count most in determining systemic reaction").

29 Alex Conte, *Security in the 21st Century: The United Nations, Afghanistan and Iraq* 23 (Ashgate 2004).

the Security Council not only mandated that countries take affirmative steps to stop the financing of terrorist acts, but it:

> *Decide*[*d*] *also* that all States shall:
>
> . . .
>
> (b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;
>
> (c) Deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens;
>
> (d) Prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens;
>
> (e) Ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts; [and]
>
> (f) Afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings.[30]

The word "[*d*]*ecide*[*d*]" carries special significance because "[t]he Members of the United Nations agree to accept and carry out the *decisions* of the Security Council in accordance with the [UN] Charter."[31] Practically every country in the world is a UN member, and thus held to the Security Council's decisions.[32] This includes the decisions announced in Resolution 1373.

Resolution 1373 thus creates an international law duty upon states to take the steps listed above. In other words, all countries must try to prevent terrorist acts. But if this fails, all countries must aid by collecting evidence, and must either prosecute or extradite any perpetrators located within their territory.

---

30 Resolution 1373, UN Security Council, 4385th mtg (Sept 28, 2001), UN Doc S/RES/1373 (specifying eleven steps for all states to take against terrorist acts).

31 UN Charter Art 25 (emphasis added) (memorializing a central function of the Security Council).

32 One hundred and ninety-two countries are UN members. See United Nations, *Member States of the United Nations*, online at http://www.un.org/members/list.shtml (visited Nov 21, 2009) (listing all 192 Member States). This includes all states recognized by the United States, excluding only the Holy See and Kosovo. See US Department of State, *Independent States in the World*, online at http://www.state.gov/s/inr/rls/4250.htm (visited Nov 21, 2009) (listing 194 states alongside their UN status). The question of whether Security Council decisions bind non-member states or non-state entities is outside of this Comment's scope.

III. CYBERTERRORIST ACTS

The recent experiences of Russia, Estonia, and Georgia demonstrate that cyberspace can quickly become a battleground in an international dispute.[33] Based on these experiences and on the growing importance of the internet to society, it seems likely that cyberattacks will become more prevalent in the future. Although the world has witnessed examples of cyberattacks, it has been relieved thus far from suffering a clear-cut cyberterrorist act.[34] As such, this Comment is unable to point to any real-world example of a cyberterrorist act. But the mere lack of an example should not foreclose the analysis, for law is often meant to be both backward- and forward-looking. In order to contemplate the cyberterrorist scenario that exists on the horizon, this Comment explores the likely conduct of tomorrow's affected, as yet unidentified, states.

Suppose a state—let's call it "Lilliput" for now—is the victim of a cyberattack so horrific that it directly causes the death of numerous civilians. Further, suppose that Lilliput has good reason to believe the cyberattack was launched from a neighboring country—called "Brobdingnag" for the time being—with which Lilliput has been involved in an ongoing and contentious row.[35] How can, and how should, both Lilliput and Brobdingnag respond to this cyberattack in a manner consistent with international law?

Lilliput will probably experience two related, kneejerk reactions. On one hand, it will need to label the attack. Was it an act of crime, an act of terror, or an act of war? On the other hand, it will want to identify the perpetrators who initiated the attack. While Lilliput will approach these issues simultaneously, this Comment can address only one at a time. Section III.A focuses on how to describe the attack. Although there is no satisfactory definition of "cyberterrorism" or "cyberterrorist act," this Section illustrates for the reader what sorts of cyberactions could qualify conceivably under these terms. Section III.B considers the question of who initiated the attack. Identifying the attacker will entail numerous investigatory steps, and will probably succeed only if other states cooperate in the investigation.

---

33 See Section I (introducing these disputes).

34 Although cyberattacks targeted Estonia and Georgia, see notes 1–4 and accompanying text, neither of these attacks would qualify as a "cyberterrorist act" under the assumption spelled out in Section III.A because neither was universally identified as such. Outside the bounds of that assumption, this Comment takes no stance on whether these cyberattacks actually were "cyberterrorist acts" under alternate definitions.

35 In *Gulliver's Travels*, "Lilliput" and "Brobdingnag" represent, respectively, undersized and oversized nations. See Jonathan Swift, *Gulliver's Travels* 51, 56, 119, 122–23 (Penguin 1985) (Peter Dixon and John Chalker, eds). Here, Lilliput and Brobdingnag represent, respectively, the victim state and the host state.

Once the attackers have been identified, Lilliput will surely want to ascertain whether Brobdingnag or any other state had a hand in the cyberattack. In spite of its suspicions, Lilliput will find it nearly impossible to attribute the cyberattack to a state because, as Section III.C establishes, state attribution still requires fulfilling the burdensome "effective control" test. This highlights a gap in state duties to prevent or respond to a cyberterrorist act, pointing the way towards the simple proposal discussed in Section IV.

A. Definition

This Comment operates under the assumption that the Security Council and international community will identify especially horrific cyberattacks as "terrorist acts." For example, a cyberattack that intentionally caused the Three Gorges Dam to flood the surrounding Chinese population would presumably be labeled a "terrorist act."[36] This assumption is necessary for two reasons. First, defining "terrorism" has proved so elusive in the concrete world that there is no basis for believing this Comment can define it as applied to the virtual world. This Comment cannot hope to succeed where generations of world leaders have failed. Second, even if this Comment could articulate a workable definition, it would quickly grow stale given the internet's rapid change and society's progressive reliance on cyberspace.[37] What makes sense today may appear folly tomorrow. This is not to deny that defining "cyberterrorism" or "cyberterrorist acts" may be possible in the future, but a workable definition will be more feasible once the degree of change tapers off a bit.

Assuming away these definitional difficulties does not undermine the implications of this Comment. True, there will be bickering over whether specific, mid-level cyberattacks qualify as "terrorist acts." It appears, though, that no such debate will take place after extreme cyberattacks, especially if they have salient, real-world effects. The September 11 response shows that the Security Council and international community are able to identify truly egregious terrorist

---

36 Such an attack would certainly be catastrophic. "Over 360 million people live within the watershed of the Yangtze River [which is damned by the Three Gorges Dam]. If the one in one thousand chance of a dam collapse occurred, the millions of people who live downstream would be endangered." PBS, *Great Wall Across the Yangtze: Facts & Figures*, online at http://www.pbs.org/itvs/greatwall/dam1.html (visited Nov 21, 2009). It is difficult to determine whether a cyberattack against the Three Gorges Dam is technically possible, but it at least seems feasible. See Xinhuanet, *Closure of Sluice Gate at Three Gorges Dam Successful*, Xinhua News Agency (June 1, 2003), online at http://news.xinhuanet.com/english/2003-06/01/content_898069.htm (visited Nov 21, 2009) (reporting that the reservoir's water level had been successfully raised "through computer-controlled operations" of most of the water diversion holes).

37 "When circumstances are changing, rules are likely to be inaccurate." Cass R. Sunstein, *Problems with Rules*, 83 Cal L Rev 953, 1015 (1995) (continuing that under "these circumstances it may be best . . . to allow case-by-case judgments based on relevant factors").

acts as such, even in previously unseen circumstances. This permits the assumption that there will always be a similar method, however crude, for all states to differentiate cyberterrorist acts from other cyberactions, at least in the most extreme examples.

Still, it may be helpful for this Comment to address some of the possibilities for identifying a cyberterrorist act. One way would be to create an agreement that recognizes specific cyberactions as inherently cyberterrorist acts. Section II.B has shown that certain acts—such as taking hostages—are to be deemed "terrorist." Although none of these clearly encompasses cyberactions, it is conceivable that a parallel consensus will emerge that equates specific cyberactions with terrorist acts. Until this occurs, however, we can only sketch out a general framework that delineates what sorts of cyberactions might qualify as "terrorist."

Susan W. Brenner offers one plausible method for how to distinguish between different cyberactions. She divides cyberactions into three types: cybercrime, cyberterrorism, and cyberwarfare.[38] To her, cybercrime—such as online harassment, theft, or fraud—consists of "the use of computer technology . . . to engage in activity that threatens a society's ability to maintain internal order."[39] This is the same as cyberterrorism, except for its motive: "[c]rimes are committed for individual and personal reasons," while "terrorism is political."[40] But if cyberterrorism is political, so too is cyberwarfare. Their difference lies not in who commits the acts, for she contends that both individuals and states can engage in cyberterrorism and cyberwarfare.[41] Instead, the distinction is that cyberterrorism specifically targets civilians, whereas cyberwarfare does not.[42] Putting this all together, one might think of cyberterrorism as the use of computer technology to target civilians in a way that

---

38 Consider Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J Crim L & Criminol 376 (2007).

39 Id at 386 (warning societies to be vigilant of "emerging [online] activities that constitute a threat to their ability to maintain internal order," and recommending criminalization of such activities).

40 Id at 387 (recognizing these motives can be conflated, but arguing we must distinguish them because we should respond to them in different ways); see also Mohammad Iqbal, *Defining Cyberterrorism*, 22 John Marshall J Computer & Info L 397, 407–08 (2004) (concluding, after discussing eight definitions of "cyberterrorism," that "[t]he difference between cyberterrorism and other cyber attacks, such as hacking and cracking, is that the cyberterrorists are politically motivated, while other cyber attackers have non-political motives").

41 See Brenner, 97 J Crim L & Criminol at 404–05 (cited in note 38) (arguing that cyberspace permits both non-state actors and states to participate in acts of crime, terror, and war).

42 See id at 387–88.

threatens society's ability to maintain internal order, when this threat is intentional and politically motivated.[43]

How might cyberterrorists achieve this goal? Brenner points out that they could wield computer technology in three distinct ways: as a weapon of mass destruction, as a weapon of mass distraction, or as a weapon of mass disruption.[44] An example of mass destruction would occur were a cyberterorrist able to hijack and disable Lilliput's computer system running a nuclear power plant, causing a devastating nuclear explosion.[45] A cyberterrorist attack of mass distraction, on the other hand, would focus on psychological manipulation of the Lilliputian public.[46] This might be done by, say, programming all internet news programs to announce the contamination of major water sources, leading to a national panic. A related, but more subtle attack, centers on mass disruption, which aims to erode the public's confidence in its infrastructure and police powers. An example of this might be shutting down a power grid in a different Lilliputian city for thirty minutes every Monday morning.[47] Of these three types of cyberterrorist attacks, only the first (and perhaps the second) class of attack will be egregious enough to qualify unequivocally as a horrific act of terrorism.

B. Investigation, Cooperation, and Identification

Let us return to the example of Lilliput, which has just experienced a horrific cyberattack. Regardless of whether the attack is ultimately classified as an act of crime, terror, or war, Lilliputians will no doubt attempt to seek out the perpetrators. But sophisticated perpetrators would have tried to shield their true identities, leading to a multileveled game of hide-and-seek between the two sides. This Comment's scope does not allow an expansion into highly technical details of computer investigations. It does presume, however, that Lilliput will succeed in identifying the perpetrators if given sufficient and timely information by cooperating states.

---

43 This Comment does not advocate this as a definition, but merely provides it to the reader as one possible way to think about cyberterrorism. Similarly, the next paragraph contemplates cyberterrorist acts in a discussion that should not be taken to be conclusive.

44 For this creative terminology, see Brenner, 97 J Crim L & Criminol at 390 (cited in note 38).

45 See id at 390–91. Brenner asserts that although "[t]his is a viable terrorism scenario, [] it is not a cyberterrorism scenario." Id at 391. She appears to qualify this assertion, however, with the empirical assumption that "the victims would recall it as a nuclear catastrophe, not as a computer catastrophe." Id.

46 See id at 391–93.

47 See id at 393–98.

Lilliput's first step will likely be to examine its own computer networks for data indicating intrusion or tampering by the cyberattackers. Once found, Lilliput will trace this data back through various intermediate routers to identify the router that first sent the data.[48] It will then need to examine the router to determine which network's server precipitated the cyberattack. In this example, Lilliput has been able to identify the server as being located in Brobdingnag without having to encroach on Brobdingnag sovereignty.[49]

Ascertaining that the server is located in Brobdingnag does not end the analysis. The server acts as a mere staging ground for the attack, and its location demonstrates only that Brobdingnag territory was used as the launch pad.[50] Lilliput will still want to identify who used this server to launch the attack; it may also wish to determine whether Brobdingnag knew or should have known its capabilities were being used for staging grounds. To do either, Lilliput will have to examine the server's network for log files and other data that memorialize the server's activities and user IP addresses.[51] This information, in turn, can point to the actual location where the attack originated, thereby facilitating the search for the perpetrators.[52] Gathering this evidence is highly time-sensitive, for it "might be erased at any moment" by the server administrator.[53]

---

48 See Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 446–48 (Academic 2d ed 2004) (showing that data usually travels from the host computer to the destination computer through various routers). This presumes, for simplicity's sake, that the intermediate routers are located within jurisdictions made accessible to Lilliput. Intermediate routers located in hostile states are addressed briefly in note 85.

49 The router, of course, could be located in Brobdingnag or in a neighboring country. For ease of argument, this example places the router outside of Brobdingnag. Were the router inside Brobdingnag, it would merely add another layer to the next paragraph's analysis. In that case, Lilliput might need to encroach lawfully on Brobdingnag's sovereignty to analyze the router that points to Brobdingnag's possession of the server, and then re-encroach to examine the server's data.

50 See Brenner, 97 J Crim L & Criminol at 409–11 (cited in note 38) (observing that we cannot necessarily equate the launching of an attack by a Chinese server with the launching of an attack by a Chinese national). See also Demetri Sevastopulo, *Chinese Hackers Penetrate White House Network,* Financial Times 7 (Nov 7, 2008) ("A second US official said government cyber experts had determined that the attacks [on the Obama and McCain campaigns] originated from China, but he cautioned that they could not determine whether they were related to the government.").

51 Section IV.B proposes recognizing Brobdingnag's international law duty to secure and provide this information.

52 See Casey, *Digital Evidence and Computer Crime* at 441, 526 (cited in note 48) (offering network information and guidance on how to investigate computer intrusions). The IP address is analogous to a home telephone number. An IP address can be altered to throw investigators off track, but it appears that an "offender can only reconfigure his computer with another IP address on the same subnet." Id at 445. If this remains true, a cyberterrorist might be able to mask his IP address (telephone number), but not his subnet (area code). It is also worth noting that IP addresses are increasingly becoming "dynamic," meaning that they can be assigned to different users at different times. But the Internet Service Provider (ISP) usually maintains a log showing

But gathering evidence located in another country can cause problems. First, Lilliput's domestic law may hamper its ability to search for, and seize, foreign evidence. This issue arises, for example, when the United States contemplates foreign searches and faces Fourth Amendment constraints.[54] Yet this hardly seems a realistic obstacle for a victim of cyberterrorism; we should expect our imaginary Lilliput to override any domestic restraints by some legal or extralegal means.[55] A second, more intractable, sovereignty issue also seems likely to surface: Brobdingnag might assert a proprietary interest in examining the server located within its physical jurisdiction, thereby preventing Lilliput from conducting its own investigation. Such an assertion might be intended to hide Brobdingnag's role in the cyberattack, but Brobdingnag's reasons could also be more innocent, such as to prevent the transfer of its technology or to extract something of equal value from Lilliput. Were Brobdingnag to assert a sole right to inspect its server, this would not only undermine Lilliput's ability to investigate, but it would also prevent a more objective third-party from analyzing valuable evidence.

This latter problem is merely one example of the continual conflict between the principles of national sovereignty and international collaboration. Thankfully, collaboration appears likely to win out, at least as far as cyberterrorism is concerned. First, Security Council Resolution 1373 creates a duty to offer "the greatest measure of assistance" to investigations, "including assistance in obtaining evidence in [the state's] possession necessary for the [criminal] proceedings."[56] This refrain is repeated again in Section IV. But a second reason exists to believe that the world will see collaboration in this area: the exponential reliance on computer systems, coupled with increased globalization, should lead to increased worry about international cyberactions. This, in turn, should precipitate states to conclude that cooperation is in their best interest, making multilateral agreement more likely.

---

which IP addresses were assigned to which users during which times. See id at 455–56 (explaining that internet cafés might use dynamic IP addresses for efficiency reasons). These dynamic IP addresses highlight the necessity of accessing the ISP's log files in order to identify cyberterrorist actors, for there may be no other way to connect an IP address to its user at the time in question.

53 Id at 526 (discussing investigative pressures).

54 See Henry J. Perritt, Jr, *Jurisdiction in Cyberspace*, 41 Vill L Rev 1, 82–90 (1996) (identifying foreign searches as "[o]ne of the most common electronic search and seizure problems" for the United States).

55 Consider Eric A. Posner and Adrian Vermeule, *Terror in the Balance: Security, Liberty, and the Courts* 15–17 (Oxford 2007) (describing United States history as a demonstration that, in times of emergency, the executive will relax constitutional standards and the judiciary will defer to this relaxation).

56 Resolution 1373 at ¶ 2(f) (cited in note 30).

Cybercrime, for example, has long been of sufficiently prominent concern, which helps explain why the UN has been toiling towards a cybercrime resolution for over fifteen years.[57] Although the UN has yet to succeed in this task, the Council of Europe has gotten the ball rolling towards universal agreement. Its Convention on Cybercrime—which institutes a system for multistate cooperation in securing and providing data relevant to a recognized cybercrime[58]—is a shining example of international state cooperation. The Convention has forty-six state signatories, including the non-European countries of Canada, Japan, South Africa, and the United States.[59] This Convention's success holds promise for future multilateral treaties that promote international investigations over other cyberactions, including acts of cyberterrorism.

Unlike cybercrime, cyberterrorism is a fairly novel development that the world has yet to consider comprehensively. Among the host of issues to be resolved is how to ensure international cooperation between future Brobdingnags and Lilliputs. Without such cooperation, it may be legally impossible to collect the evidence necessary to identify the attack's perpetrators.[60] Section IV proposes the recognition of an international law duty that is adequate to guarantee efficient and effective investigation of international cyberterrorist acts. With such a duty recognized by international law and honored by states, Lilliput should be able to identify the perpetrators.

C. Attribution and Its Impossibly High Hurdle

Once Lilliput succeeds in identifying the cyberterrorists, it will no doubt attempt to ascertain whether they were acting alone or on behalf of Brobdingnag (or another state). This is a complicated process, but how the world resolves this issue could have serious repercussions. If Lilliput can demonstrate that the cyberattackers acted as agents of Brobdingnag, this would turn the attacks themselves into Brobdingnag state action. Would this constitute an "armed

---

57 See Susan W. Brenner and Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 John Marshall J Computer & Info L 347, 363 (2002) (stating in 2002 that "[t]he United Nations has been working towards resolving the problems raised by cybercrime for more than a decade").

58 See Convention on Cybercrime (2001), Arts 15–21, 23, 25, 27, 41 ILM 282 (2001).

59 See Council of Europe, *Convention on Cybercrime*, online at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (visited Nov 21, 2009) (showing that the Convention has already entered into force in half of these forty-six countries).

60 See Brenner and Schwerha, 20 John Marshall J Computer & Info L at 395 (cited in note 57) (stating that "[i]nternational cooperative efforts among law enforcement personnel will be [] essential" for acquiring evidence held in a foreign land).

attack," thereby triggering Lilliput's inherent right to engage in self-defense?[61] Answering this question conclusively is outside of this Comment's scope, but it seems likely that a Brobdingnag-controlled cyberattack would activate Lilliput's self-defense right, possibly sparking an armed conflict between the two states.

This issue, though, quickly becomes a moot point. Even if Lilliput can show that the cyberattack originated within Brobdingnag territory, attributing the cyberterrorists' acts to the state of Brobdingnag will prove near-impossible. For one thing, it could well be that the Brobdingnag government is innocent of having any knowledge of, or ties to, the cyberterrorists. In such a case, it would be factually and legally incorrect to attribute the cyberattacks to Brobdingnag. For another thing, the "effective control" test for attribution presents a high hurdle that is exceedingly difficult for any state to leap over.

The International Court of Justice (ICJ) first stated the "effective control" test for state attribution in the *Nicaragua* case,[62] in which Nicaragua accused the United States of directing the Contras' paramilitary activities in and against Nicaragua.[63] "For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had *effective control* of the military or paramilitary operations in the course of which the alleged violations were committed."[64] No definition of "effective control" was forthcoming but, applied to the facts of the case, it required something *more* than "financing, organizing, training, supplying and equipping of the [attackers], the selection of [their] targets, and the planning of the whole of its operation"[65] This presents a seemingly insurmountable obstacle to establishing state attribution in any case lacking a smoking gun.

The effective control test has not existed free of challenges to its overbearing standard. Most notably, the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia (Appeals Chamber) announced a lower standard for hierarchically structured groups like paramilitaries, where "the group as a whole [must be shown to] be under the *overall control* of the State."[66] The Appeals Chamber also recognized a different test for "a *single* private

---

61 Consider UN Charter Art 51 (recognizing a state's inherent right to defend itself in response to an "armed attack").

62 *Military and Paramilitary Activities* (Nicaragua v United States), 1986 ICJ 14 (June 27, 1986).

63 Id at 21–22 (laying out Nicaragua's claims).

64 Id at 65 (emphasis added).

65 Id at 64 ("All the forms of United States participation mentioned, and even the general control by the respondent State over a force with a high degree of dependency on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts.").

66 *Prosecutor v Tadić*, Case 94-1-A, 49 (ICTY App Chamber 1999) (emphasis added) (distinguishing between structured groups and individuals).

individual or *a group that is not militarily organised*": whether the state specifically instructed the perpetrator to commit the act in question, or whether the state responded to the act by offering its public endorsement or approval.[67] Regardless of whether the cyberterrorist is classified as a structured group, an unstructured group, or as a private individual, the Appeals Chamber's test appears to be more achievable than the ICJ's effective control test. But despite international respect for the Appeals Chamber, the ICJ's decision probably carries more precedential weight.[68]

The International Law Commission (ILC)—a long-standing subsidiary organ of the UN General Assembly[69]—also stepped into the fray when it released its Draft Articles on the Responsibility of States for Internationally Wrongful Acts (Draft Articles).[70] In doing so, the ILC opted to codify the ICJ's effective control test, while rejecting the Appeals Chamber's lesser, overall control standard.[71] True, the Draft Articles have yet to be accepted as binding international law.[72] But the decision to adopt the effective control test was not made lightly, as the Draft Articles were nearly forty years in the making.[73] This, combined with the ICJ's decision, leads this Comment to recognize "effective control" as the contemporary test for state attribution.

The prevailing standard of "effective control" poses such a high hurdle for attacks that it seems unlikely that Lilliput could ever attribute a cyberattack to Brobdingnag or any other state.[74] International law on attribution might catch

---

67 Id at 58–59 (presenting its holding on the law of state attribution).

68 Consider UN Charter Art 92 ("The International Court of Justice shall be the principal judicial organ of the United Nations.").

69 See Resolution 174, UN General Assembly, 123d mtg (Nov 21, 1947), UN Doc 174 (II) 105 (establishing the ILC in 1947); UN, *Subsidiary Organs of the General Assembly*, online at http://www.un.org/ga/commissions.shtml (visited Nov 21, 2009) (listing the ILC as a subsidiary organ).

70 See International Law Commission, *Draft Articles on the Responsibility of States for Internationally Wrongful Acts* at Art 12 (cited in note 5).

71 Id at Art 8 (attributing conduct to a country if the perpetrators are "in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct"). The Commentaries to the Draft Articles "also embrace the *Nicaragua* effective control standard and reject the *Tadić*, overall control standard." Chase, 45 Va J Intl L at 116 (cited in note 19).

72 See Resolution 56/83, UN General Assembly, 56th Sess (Dec 12, 2001), UN Doc A/RES/56/83 ¶3 (Jan 28, 2002) ("*Tak[ing] note* of the articles . . . and commend[ing] them to the attention of Governments without prejudice to the question of their future adoption or other appropriate action.").

73 See Chase, 45 Va J Intl L at 112 & n 382 (cited in note 19) (giving this time span).

74 For the difficulty of meeting this standard, see *Military and Paramilitary Activities*, 1986 ICJ at 65 (cited in note 62) (failing to hold the United States responsible for the Contras' actions in Nicaragua despite numerous substantive links). For a statement about the difficulty experts face in attributing a cyberattack to a state, see Sevastopulo, *Chinese Hackers Penetrate White House Network*,

up to these recent developments by lowering the standard for attributing conduct to a state.[75] In the meantime, however, another avenue should be considered for curtailing cyberterrorist acts.

IV. RECOGNIZE THE DUTY TO PREVENT AND RESPOND TO CYBERTERRORIST ACTS

International law should recognize that states have a duty to prevent and respond to cyberterrorist acts. Security Council Resolution 1373 created a similar duty regarding terrorist acts, and this should be expanded into the frontier of cyberspace. There will remain definitional disputes over what cyberacts qualify as "terrorist," but this should limit only the strength of the forward-looking duty to prevent cyberterrorist acts. Defining the cyberact as "terrorist" must take place before the duty to respond to cyberterrorist acts arises, meaning that states cannot circumvent this backward-looking duty through semantics. This duty to respond, once triggered, has two implications for all states: they must cooperate with criminal investigations by providing evidence, and they must bring to justice alleged cyberterrorist actors by arresting them and either prosecuting or extraditing them. Thankfully, states have already accepted these implications in similar situations, so the recognition of this duty should not further overburden states.

A. Security Council Resolution 1373 Should Apply to Cyberterrorist Acts

The Security Council passed its wide-ranging Resolution 1373 only a few weeks after September 11. Because the Resolution contains the word "*[d]ecides*," it obligates all 192 UN member states to carry out the Security Council's "decisions" announced therein. Thus, Resolution 1373 creates binding international law.[76]

What decisions, then, did the Security Council express in the Resolution? Section II.C provides the most pertinent decisions verbatim, but it is worth recapping them here. All states have an ongoing duty: 1) to try to prevent terrorist acts, in part by sharing information with other states, 2) to prevent their territories from harboring anyone associated with terrorist acts, 3) to prevent

---

Financial Times at 7 (cited in note 50) ("US government cyber experts suspect the attacks [on the White House] were sponsored by the Chinese government, although they cannot say for sure.").

75 Consider Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 Chi J Intl L 83, 90 (2003) (observing a relaxation of the strict attribution standard in favor of an emerging proscription of harboring or supporting terrorists).

76 See notes 30–32 and accompanying text.

their territories from being used for committing terrorist acts, and 4) to ensure their domestic laws sufficiently criminalize and punish terrorist acts.[77] But that is not all. If this fails to prevent terrorist acts, then all states must: 1) aid in bringing any participants to justice, and 2) do their utmost to help the investigations and criminal proceedings, including helping to obtain evidence in their jurisdiction.[78] These two duties comprise, respectively, the duty to prevent and the duty to respond.

It should be readily apparent when looking at Resolution 1373 that the threshold question, at least in theory, becomes what acts should be termed "terrorist." Thirteen instruments list distinct acts that are automatically considered "terrorist" by the international community, but the response to September 11 showed that the Security Council and the world do not need to rely upon such instruments to label extreme attacks as "terrorist." Instead, they can apply this label the very next day in radical, previously unseen circumstances.[79] As a result, this Comment assumes that no definitional problem will exist after a truly egregious terrorist attack, including a novel cyberterrorist attack.[80] That is, a cyberterrorist act will be deemed a "terrorist act" in the most extreme cases.

Although Resolution 1373 does not address cyberterrorism, it should be interpreted to encompass cyberterrorist acts. It is no accident that, out of the almost two thousand Security Council resolutions,[81] Resolution 1373 is "one of the most strongly worded resolutions in the history of the Security Council."[82] A quick look at the excerpted portion in Section II.C should confirm that its language is both strong enough and broad enough to establish a state's duty vis-à-vis cyberterrorist acts.[83] This should prove uncontroversial, especially if any definitional issue is set aside. It should be recognized that states have an international law duty to prevent or respond to cyberterrorist acts, when they are identified as such.

---

77 See Resolution 1373 at ¶¶ 2(b)–(e) (cited in note 30).

78 See id at ¶¶ 2(e)–(f)

79 See Sections II.B–II.C (discussing these international agreements and the international response on September 12, 2001).

80 See Section III.A (announcing this assumption).

81 Through October 2009, the Security Council had passed 1893 resolutions. See UN Security Council, *Resolutions 2008*, online at http://www.un.org/Docs/sc/unsc_resolutions09.htm (visited Nov 21, 2009) (listing the 1893rd Security Council resolution).

82 Conte, *Security in the 21st Century* at 23 (cited in note 29).

83 See note 30 and accompanying text (providing a significant portion of this impressive resolution).

B. Reasonable Implications for All States

This duty, once recognized, holds a handful of reasonable implications for all 192 UN member states. But much as the duty itself is divisible into two categories—the duty to prevent and the duty to respond—the real-world implications also divide into two types of varying strength. The duty to prevent is a permanent obligation but, because states can reasonably diverge on what future acts will be "cyberterrorist" and so can circumvent the spirit of the duty, it is also a weak duty. Conversely, the duty to respond arises only after an egregious cyberact has already been deemed "cyberterrorist." This duty may arise only occasionally, but it is relatively strong because no definitional circumvention is possible. Table 1 illustrates this dichotomy.

The duty to prevent is a permanent duty, so all states always have the obligation to: 1) try to prevent cyberterrorist acts, 2) prevent their territories from harboring cyberterrorist associates, 3) prevent their territories from being used as launching pads for cyberterrorist acts, and 4) ensure their domestic laws adequately criminalize and punish cyberterrorist acts. These duties are forward-looking, meaning that every state must perform them in the hopes of preventing future cyberacts that are "terrorist" in nature.

Type of Duty	When Is the Duty Created?	Duties	How Is "Cyberterrorist Act" Defined?	Relative Strength of Duty
Duty to Prevent	Immediately	1. Try to prevent cyberterrorist acts, in part by sharing information 2. Prevent territories from harboring associates of cyberterrorist acts 3. Prevent territories from being used to commit cyberterrorist acts 4. Ensure domestic laws sufficiently criminalize and punish cyberterrorist acts	Each individual state considers any reasonable definition it wishes to apply to future cyberattacks → States have significant wiggle room to define according to their interests	Weak, but Permanent
Duty to Respond	After a cyberattack has occurred, and after it has been deemed a "terrorist act"	1. Help bring to justice any cyberterrorist actors 2. Do whatever is necessary to aid criminal investigations and proceedings, including securing evidence	The Security Council and/or international community has already defined a cyberattack as a "terrorist act" → States have no wiggle room to define according to their interests	Strong, but Sporadic

Table 1: A State's Duty to Prevent and Respond to Cyberterrorist Acts

Cyberacts, though, do not fall clearly under one of the thirteen conventions proscribing terrorist acts, so a "cyberterrorist act" must be determined on an ad hoc basis. This makes it impossible to classify in advance what specific acts will qualify as "cyberterrorist." Every state, therefore, enjoys significant wiggle room to adopt a definition of "cyberterrorist act" that best suits its interests, so long as the definition is reasonable. For example, states with strong tourist economies might focus on the cybertargeting of tourists, states with stock markets could fret about a cybercrash, and states with limited resources may focus on even

more limited notions of "cyberterrorist acts." This might lead to a patchwork of domestic laws and preventative measures aimed at curtailing varying ideas of as-yet-unseen "cyberterrorist acts." Despite the duty to prevent cyberterrorist acts, we should not expect states to implement it in a way that palpably improves world prevention.

If the duty to prevent is permanent, forward-looking, and weak, then the duty to respond is sporadic, backward-looking, and strong. This latter duty entails: 1) helping bring to justice any cyberterrorist actors, and 2) aiding criminal investigations and proceedings by securing evidence and other means.

Significantly, the duty to respond materializes only after a "cyberterrorist act" has occurred. This happens when there is a cyberattack *and* when it is universally identified as a "terrorist act." Recall that, in the most extreme cyberattacks, this identification will presumably take place almost immediately, much like the next-day response to September 11. Once identified as such, this cyberterrorist act triggers the duty of all states to respond to it. Because the act has already been defined as "cyberterrorist," states can no longer quibble over the definition, and thus cannot avoid their duty through semantics. The duty to respond may arise sporadically but, once it does, states cannot minimize its importance.

1. States must cooperate with criminal investigations by providing evidence.

Most importantly, the duty to respond sets up a regime where all states must cooperate with criminal investigations and proceedings by providing relevant evidence. This duty to cooperate comes from Resolution 1373's decision "that all States shall . . . [a]fford one another *the greatest measure of assistance* in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings."[84] So the Brobdingnags of the world (and every other state) must do everything they can to help the Lilliputian investigation into the cyberterrorist act it suffered. Lilliput, in Section III.B, needed to inspect data on the server located in Brobdingnag's jurisdiction.[85] Brobdingnag must do its utmost to aid in this inspection, which

---

84 See Resolution 1373 at ¶ 2(f) (cited in note 30) (emphasis added) (announcing this duty).

85 See notes 50–52 and accompanying text (discussing why this inspection will help Lilliput deduce the server's activities and user IP addresses necessary to identify the perpetrators' location and, hopefully, the perpetrators). This example assumed, for ease of argument, that Lilliput encountered no problem tracing data from its own computer network to Brobdingnag's server through various intermediate routers. See note 48 and accompanying text. Even if these intermediate routers are located in states hostile to Lilliput, those states have the same duty to

includes securing the network's time-sensitive evidence and providing it to the investigators.

This obligation to cooperate enjoys significant overlap with the Convention on Cybercrime, making the obligation appear especially workable. Section III.B introduced this Convention as a multilateral treaty with forty-six state signatories that have already agreed to the Convention's terms.[86] Chief among those terms is a "general principle" that all signatories must "afford one another mutual assistance to the widest extent possible for the purpose of investigations or [criminal proceedings] . . . or for the collection of evidence in electronic form of a criminal offense."[87] This language tracks that of Resolution 1373,[88] and the sheer fact that so many states have voluntarily agreed to this principle speaks to its feasibility. Of course, the Convention specifies other terms, such as telling states how to request the preservation of data, and requiring states to set up an always-available point of contact.[89] These additional terms have no explicit corollary to the wide-ranging international law obligation recognized here, but they might provide useful guidance for determining whether states have fulfilled their international law duty to offer "the greatest measure of assistance" required by Resolution 1373.

2. States must arrest, and prosecute or extradite, accused cyberterrorist actors.

The duty to respond also obliges states to arrest, and prosecute or extradite for prosecution, anyone accused of being associated with a cyberterrorist act. Resolution 1373 compels all states to "ensure that any person who participates in [or supports] . . . terrorist acts is *brought to justice.*"[90] Although Resolution 1373 does not define "brought to justice," other Security Council resolutions equate it

---

respond to a cyberterrorist act, and so would have to cooperate in Lilliput's investigation by securing and providing relevant evidence on the intermediate routers.

86 See notes 58–59 and accompanying text (describing the Convention on Cybercrime as a shining example of international cooperation aimed at combating an early and continuing species of cyberattacks).

87 Convention on Cybercrime, Art 25(1) (cited in note 58).

88 This is unsurprising, given that the Convention on Cybercrime adopted this language less than two months after the Security Council passed Resolution 1373. Compare Council of Europe, *Convention on Cybercrime* (cited in note 59) (showing the Convention was first opened for signature on November 23, 2001), with Resolution 1373 (cited in note 30) (Sept 28, 2001).

89 Convention on Cybercrime (cited in note 58), Arts 29–30 (establishing the procedure to request the preservation of data), Art 35 (requiring states to designate a point of contact that will be available at all times).

90 See Resolution 1373 at ¶ 2(e) (cited in note 30) (emphasis added) (announcing this duty).

with "the principle to extradite or prosecute."[91] This means that the arresting state can either prosecute the alleged cyberterrorist actor in its own courts, or it can extradite him or her for prosecution elsewhere. Because Resolution 1373 also commands states to establish terrorist acts "as serious criminal offences in domestic laws . . . [so] that the punishment duly reflects the seriousness of such terrorist acts,"[92] the arresting state should meet its duty to "bring to justice" accused cyberterrorist actors regardless of whether it opts to prosecute or extradite them.

This regime is already commonplace in international law concerning terrorist acts, so it should prove just as workable in relation to cyberterrorist acts. Of the thirteen UN-recognized instruments defining "terrorist acts," most "obligate all member states to make the offense a crime under their domestic law, and impose a try-or-extradite obligation on all states with respect to persons found in their territory alleged to have committed the offense."[93] This duty to arrest, and extradite or prosecute, accused cyberterrorist actors is no different, and therefore should prove just as reasonable as other agreed-upon duties.

V. CONCLUSION

Cyberterrorism, in all forms, appears ready to pose an acute problem for the future. As society continues its globalization process, it will rely ever more upon networked systems, and this technology will become ever more accessible to hostile individuals. To the extent that cyberterrorists commit cross-border attacks, international law will be at the forefront of responding to cyberterrorism.

---

91 Resolution 1566, UN Security Council, 5053d mtg (Oct 8, 2004), UN Doc S/RES/1566 at ¶ 2 (calling upon all states "to find, deny safe haven and bring to justice, on the basis of the principle to extradite or prosecute" anyone participating or attempting to participate in terrorist acts); Resolution 1456, UN Security Council, 4688th mtg (Jan 20, 2003), UN Doc S/RES/1456 Annex at ¶ 3 ("States must bring to justice those who finance, plan, support or commit terrorist acts or provide safe havens, in accordance with international law, in particular on the basis of the principle to extradite or prosecute."). The Chair of the Counter-Terrorism Committee wrote a report that, confusingly, interprets Resolution 1373 to require states to try alleged terrorists, while also observing that states would be competent to try or extradite them. See *Report by the Chair of the Counter-Terrorism Committee on the Problems Encountered in the Implementation of Security Council Resolution 1373* (2001) 6 ("[Resolution 1373] obliges States to prosecute and try all those responsible for acts of terrorism, wherever they are committed. This measure is designed to ensure that terrorists have no place of refuge, since each State will be competent to try them or extradite them."), annexed to *Note by the President of the Security Council*, UN Security Council (Jan 26, 2004), UN Doc S/2004/70. This Comment opts to follow the more persuasive interpretation given by the Security Council.

92 See Resolution 1373 at ¶ 2(e) (cited in note 30) (announcing this duty as well).

93 Carter, Trimble, and Weiner, *International Law* at 1172 (cited in note 7) (discussing the international consensus when it comes to specific acts of terror and what must be done to punish their perpetrators).

Sharing this forefront will be state cooperation. In an ideal world, all states would simply agree to prevent or respond to cyberterrorist acts. But then again, in an ideal world, we might not need law at all. For now, the best option we have is to recognize that Security Council Resolution 1373 has created an international law duty that requires all states to prevent and respond to cyberterrorist acts.

Recognizing this duty will, at first, cause few real-world changes. This is because the duty to prevent is relatively flexible, owing to states' abilities to define "cyberterrorist act" to meet their varied interests. But once the world suffers its first cyberattack that is so horrific it provokes universal identification as a "terrorist act," we should expect the duty to respond to play a crucial role in international law. Recognition of this duty is a prerequisite for applying it in such dire circumstances.

CJIL