Designation of North Korea as a State Sponsor of CyberTerrorism,
On

Justin L. Koplow

Recommended Citation

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in SMU Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
On Designation of North Korea as a State Sponsor of CyberTerrorism

Justin L. Koplow*

I. INTRODUCTION

There are ample reasons to be wary of labeling an event an act of “cyberterrorism.” For too long the term has been employed as both a dodge and a hustle; the former by those who minimize the importance of investing in cybersecurity until confronted with a “cyber 9/11” and the latter by those fear-mongering beyond all reasonable limits to obtain enormous sums of security dollars. While clearly one must watch his wallet either way when “cyberterrorism” is invoked, what is less clear is the meaning of the term, itself. Indeed, although coined some thirty years ago, cyberterrorism has many definitions, which means it really has no single accepted definition. The basics seem clear enough—use of computer networks to perpetrate harm and incite terror—but the devil is in the details. Must the attackers have an ideological motivation? Must non-state actors commit the act? Must the target of the harm be a civilian population? Most fundamentally, what constitutes terror in an artificial world?

And so, “cyberterrorism” sputters along, loved, feared, and misunderstood. However, as will be explored later in this article, several recent incidents suggest a developing and growing trend of what seem to be ideologically motivated cyberattacks, intended to change the behavior of the attack targets or society and, in some cases, cause serious damage in the process.

The 2014 hack of Sony Pictures Entertainment (Sony) is the most notorious example of this trend. From that attack, gallons of digital ink were spilled and consequences both serious and hilarious abounded. We learned that Channing Tatum sends emails IN ALL CAPS; at least one executive lost her job; viewing a terrible movie briefly became a defiant political act; reams of employee health information were made public, forming the basis of class action litigation; and sanctions were imposed upon North Korean entities via

* The author is an attorney with AT&T in Dallas, Texas. He worked previously for the U.S. Intelligence Community; however, the views expressed in this article are those of the author, alone, and do not reflect the opinions or policies of either AT&T or the U.S. Government. This article adapts and expands upon a presentation the author gave to the Cyber-Security Symposium hosted at Southern Methodist Law School on October 23, 2015.

1. Compare Thomas Rid, Cyber War Will Not Take Place, 35 J. OF STRATEGIC STUD. 5, 5 (2012) (arguing that “it is unlikely that cyber war will occur in the future”), with Richard Clarke & Robert K. Knaake, Cyber War: The Next Threat to National Security and What to Do About It 103 (2010) (Clarke speculates that a cyberattack could “disable trains . . . blow up pipelines . . . cause blackouts and damage electrical power grids . . . wipe out and confuse financial records . . . disrupt traffic in urban areas . . . wipe out medical records . . .”).
Executive Order. But while these actions were undeniably "cyber," the only official invocation of "terror" was by the hackers themselves. Perhaps that should change.

That is the central idea of this article: not to settle the effort to define the term "cyberterrorism" (for that work is well set by the likes of Barry Collin, Dorothy Denning, Jim Lewis) but rather to propose a novel application of the concepts in practice. Specifically, this article proposes a designation of North Korea as a State sponsor of terrorism explicitly on the basis of its support for the hacking of Sony, which constitutes an act of terrorism.

Section II of this article considers the elements of "cyberterrorism" under U.S. law to find a commonality of approaches and reviews examples to help understand the combined term. Section III summarizes the relevant facts of the hack of Sony Pictures and applies these facts to the underpinnings of cyberterrorism. Section IV reviews the United States' process for designating a State as a sponsor of terrorism. Section V proposes that returning North Korea to the State sponsors of terrorism list—relating explicitly on its involvement in the Sony attack—would being to establish how "cyberterrorism" would actually be used in State practice and then concludes with consideration of the effects of such action.

II. TERRORISM BY ANY OTHER NAME

A portmanteau of two of the buzziest, most abused terms in modern use, it is instructive to look at each component piece before considering what is—and the larger world of what is not—cyberterrorism.


A. On Terror

Maximilien Robespierre explained, at the height of the Reign of Terror, that "terror is nothing other than justice, prompt, severe, inflexible." More recently, a saying has emerged that "one man’s terrorist is another’s freedom fighter." These statements offer several points central to understanding the term "terrorism."

i. Terrorism Requires Intentional Disruption

Robespierre’s backdrop was thousands of executions by guillotine. The second quote references a freedom “fighter,” not a freedom “ballot-measure initiator.” One does not simply initiate an act of terror by accident; it is calculated, intended to cause disruption.

ii. Terrorism Pits a Group Against the Society and/or the State

Although the passage of time between these two quotes captures the historical switch from the State as perpetrator of terror to an individual or minority group in that role, in modern times, terrorism is a tactic of asymmetric warfare—how the “little guy” strikes a serious blow on the masses. Incorporating the above, the terrorist’s activity disrupts society.

iii. Terrorism is Ideologically Motivated

Looking to the second quote, the notion of “freedom” fighter is a placeholder for any cause: religion, political, societal, and so forth. Financial or even emotional causes are more likely to be considered crime than terrorism. The fundamental point is that the terrorist actor has a larger motivation, and the act of terrorism is intended to further that motivation. Incorporating the above, the terrorist’s activity disrupts society in pursuit of the terrorist’s ideological motivation.


8. See, e.g., Molly J. Hall, MD, et al., Psychological and Behavioral Impacts of Bioterrorism, PTSD RESEARCH QUARTERLY (Fall 2002), http://www.ptsd.va.gov/professional/newsletters/research-quarterly/v13n4.pdf (noting “the primary goal of terrorism is to disrupt society by provoking intense fear and shattering all sense of personal and community safety”).


10. Id.
Moving from the theoretical to the practical, there are multiple definitions of "terrorism" in U.S. law alone. Their sources include the Code of Federal Regulations, the Department of Defense, the Federal Emergency Management Agency, and the Terrorism Risk Insurance Act each offering an interpretation of the term. But for instant purposes, the two most salient definitions are those used by the Department of Justice in Title 18 and the Department of State in Title 22.

Title 18 of the U.S. Code defines both "international terrorism" and "domestic terrorism." The two definitions are identical but for where the underlying acts occur. Thus, "international terrorism" criminalizes activities that:

(A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;

(B) appear to be intended—
   (i) to intimidate or coerce a civilian population;
   (ii) to influence the policy of a government by intimidation or coercion; or

---

11. International law has attempted to define terrorism base on prohibition of certain activities, such as airplane hijacking or terrorist financing, versus a holistic approach.

12. 28 C.F.R. § 0.85(1) (2015) (defining terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.").

13. Joint Chiefs of Staff, Washington D.C., Joint Pub. 3-07.2, ANTITERRORISM (Nov. 24, 2010), at vii, https://www.hsdl.org/?view&id=753152 (defining terrorism as "the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political.").


16. See 18 U.S.C. § 2331 (2012) (notably, the definition of domestic terrorism was added only after the terrorist attacks of September 11, 2001, through Section 802 of the USA PATRIOT Act of 2001).

17. See id.
(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

(C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum;¹⁸

This definition clearly requires (1) disruptive, illegal acts such as “mass destruction, assassination, or kidnapping,” where those involved have (2) an intention to, or at least the appearance of an intention (3) to intimidate, coerce, influence, or affect the conduct of (4) either a “civilian population” or a “government.”¹⁹ These align with two of the elements mentioned above, but Title 18, however, does not address an ideological motivation requirement, speaking to only general mens rea of “intentional” act to intimidate, regardless of the actor’s agenda.²⁰

A second provision of U.S. law picks up that thread. Section 2656f of Title 22 of the U.S. Code defines “terrorism” as “premeditated, politically motivated violence against noncombatant targets by subnational groups or clandestine agents.”²¹ Beyond adding an ideological motivation, this definition restricts the target set to “noncombatants” and the actors to “subnational groups” or “clandestine agents.”²² These elements of the definition serve, principally, to distinguish acts of terrorism, committed by non-state ideologues, from acts of war, reserved to state actors.²³

B. On Cyber²⁴

The most relevant treatment of “cyber” activity in U.S. law is Section 1030(a)(5); it criminalizes damage resulting from computer use.²⁵ In three related crimes, this section addresses one who:

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

¹⁸. Id.
¹⁹. Id.
²⁰. See id.
²². See id.
²³. See id.
(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.26

When comparing the factors underlying terrorism and the elements of Section 1030(a)(5) the most obvious commonality is that of causing disruption. This is not a surprise; both Sections 2331 and 1030(a)(5) define crimes under U.S. law, the systemic approach for which requires elements of mentality and activity. But Section 1030(a)(5) also shares with terrorism at least a notion of pitting the actor against a larger group, as all three crimes require the actor to proceed "without authorization."27 Exclusion from a group (by denying authorization) is a means of creating the minority-majority relationship. Exceeding given authorization, thus, attacks the majority group. Examining these commonalities begins to show how "cyber" and "terrorism" may be melded into a single act.

Section 1030(a)(5) does not speak to any requirement that the actor had ideological motivations or was part of a non-state entity. It does, however, foreshadow questions about the nature of the resulting damage. While the crimes outlined in Section 1030(a)(5) initiate as misdemeanors, if the activity results (or would have resulted if the activity were completed) in certain types of damage, the crime becomes a felony.28 These damages are:

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

26. Id.; Prosecuting Computer Crimes, supra note 24 at *24 ("Protected computer" is defined in the CFAA, but, in practice, means any computer connected to the Internet).

27. See id.

(VI) damage affecting 10 or more protected computers during any 1-year period.29

Interestingly, II, III, and IV are “real world” damages, specifically to a person’s health care, to a person’s body, or to public health and safety.30 But the remaining three could conceivably manifest in only the cyber world.31 For example, the loss of $5,000 or more could result from damage to computer hardware or software or the loss of intellectual property; damage to a U.S. government computer in administration of national security could result from taking such a computer offline through technical disablement; and damage to ten or more protected computers could result from damage to hardware or software or network infrastructure that denies the services of such computers.32 These damages would be legally sufficient, even if the affected computers are not physically destroyed or damaged.

Pulling these underlying concepts together, one can create a joint list of factors that underpin “cyber” and “terrorism” to include: (1) disruptive, illegal acts; (2) intent to influence behavior; (3) the minority/majority relationship; (4) an ideological motivation; (5) restriction to sub-national actors; and (6) the possibility that damage not manifest physically in the real world.

C. On Cyberterrorism

It is the last of these factors, the possibility that damage may not manifest physically, that has proven the most divisive because the ability to cause sufficiently terroristic effect without damage in the physical world is a relatively recent development. Consider the statement of Professor Dorothy Denning to define “cyberterrorism” in 2000:

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that

29. Id.
30. Id.
31. See id.
32. See id.
Professor Denning’s statement was, and remains, a leading definition of cyberterrorism. However, it was an opinion rendered in 2000 when the technological landscape was quite different. In such a context, one could hardly imagine the value of assets that exist entirely outside the real world and the destructive, even terroristic value of their deprivation or removal. But in the modern world where whole communities and businesses, such as Facebook or cloud storage providers, have untold riches in intellectual property and electronic documents that exist solely online, it becomes more conceivable to have a terrorist act that does not have any manifestation in the real world. A definition ascribed to the Federal Bureau of Investigation (FBI) comes closest to envisioning non-physical damage. Mirroring Title 22, Section 2656f, this definition posits “cyberterrorism” as “premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.”

To test these factors as underlying cyberterrorism, consider three examples of recent cyber events to determine whether they are “cyberterrorism” or another kind of cyber activity:

1. In 2007, “cyberterrorists” hacked the power grid, air traffic control, broadcast media, the stock market, elevator shafts, telecommunications networks, and other targets. If you somehow missed all of

---

33. 28 C.F.R. § 0.85(1) (2015) (defining terrorism as “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”).

34. See id.

35. However, Harold Koh, then State Legal Adviser to the U.S. State Department, commented that a cyber activity “would likely be viewed as a use of force,” pursuant to Article 2.4 of the UN Charter, where the activities “proximately result in death, injury, or significant destruction.” Significantly, Koh did not claim such real world damage is a per se necessary factor and the consideration for “use of force” should merit a higher threshold; nor was Koh specifically addressing U.S. law or terrorism. Harold Koh, Legal Adviser to the U.S. State Dep’t, “International Law in Cyberspace” at USCYBERCOM Inter-Agency Legal Conference, (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.


37. See id. (emphasis added); see also 22 U.S.C § 2656f.

this, it is the plot to “Live Free or Die Hard,” in which Bruce Willis manages to stop this cyberattack by shooting it. But Hollywood is often an early adopter of our worst fears. Although the “terrorist” professes an ideological motivation—namely showing the world that reliance on technology makes us massively vulnerable to malicious actors—he is, at the end of the day, actually looking to steal billions of dollars. While some would say greed is an ideological motivation, the law would more readily categorize these events as cybercrime rather than true cyberterrorism, as addressed under Title 18, Section 1030.

2. In 2008, tensions flared in the South Ossetia region of Georgia, bordering Russia. In advance of an actual shooting war, cyber actors hit a number of websites of the Georgian Government with distributed denial of service (DDOS) attacks and defacement campaigns. The targets included the website of the Georgian President Mikhail Saakashvili, of whom several pictures were set in comparison to similar images of Adolph Hitler. While certainly a cyber activity with ideological motivations—given the larger context of the brewing military conflict and the hackers’ likely association, or at least alignment, with, the Russian Government—the activity against Georgia would more likely be categorized an act of war. In this case, the activity was akin to propaganda or psychological operations to undermine the enemy’s will to fight, thus falling outside the limitations of Title 22, Section 2656f.

3. Recent years have witnessed the growth of the self-proclaimed Islamic State of Iraq and Syria (ISIS) and particularly its savvy exploitation of social media. In addition to a claimed hack of U.S. Central Command’s Facebook page, the group has Twitter feeds, an encrypted chat app, and makes frequent and often gruesome use of

39. Id.
40. Id.
43. Id.
44. Id.
YouTube. An argument could be made that YouTube videos of beheadings are intended to intimidate the public into changing policy; however, if these activities principally aim to inspire others to join ISIS, to take up the cause individually, to fundraise, or to communicate, both to members or to the world, such activities would be considered adversarial use of the internet, but not true cyberterrorism pursuant to either Sections 2331 and 1030.

However, two recent examples that more likely would be considered cyberterrorism:

1. In 2008, the hackers of Anonymous and 4Chan started a harassment campaign against the Church of Scientology in response to perceptions that the Church was attempting to censor or restrict embarrassing information online. The tools used in what has come be known as “Chanology” were both cyber and real world, including DDOS attacks and black faxes, as well as sit-ins and petitioning the IRS for investigation. There was clearly ideological motivation; Anonymous believes, unrelentingly, that all information should be free for all. The attacks were intended to force a group—the Church of Scientology—to change its behavior, and the modus operandi was cyber-enabled.

2. 2015 saw the release of accounts registered on Ashley Madison, a website that catered to (almost exclusively) married men seeking to have affairs. A group calling itself the “Impact Team” hacked the servers of Ashley Madison’s parent company and then attempted to blackmail the company into shutting down on belief that the company was trading in sin. When the company did not comply, the Impact Team released the information. This attack was clearly ideologically motivated and clearly accomplished via cyber means, but even more so than Chanology, pushed the limits of “damage.”

47. Id.; Josh Constine, ISIS Has Its Own Encrypted Chat App, TECHCRUNCH (Jan. 16, 2016), http://techcrunch.com/2016/01/16/isis-app/.
50. Id. at 71.
51. Id.
52. Id.
54. Id.
55. Id.
Which brings us to the biggest recent example, the 2014 hack of Sony Pictures Entertainment.

III. MAKING JAMES FRANCO A CHAMPION OF FREE SPEECH

On November 24, 2014, the world became aware of what Sony had known for some time: there was a major hack. That morning, Sony employees booted computers to an image of a red skeleton and the banner announcement “Hacked by GOP.” The group claiming responsibility, the Guardians of Peace, threatened to release a claimed 100 terabytes of Sony’s internal data, including unreleased draft scripts of full-length films, movie star salary information, internal emails, and personal information, including health information of Sony employees. When Sony balked, the Guardians of Peace


58. Peterson, supra note 57; Seal, supra note57; Grisham, supra note 57; Betters, supra note 57; Ragan, supra note 57; Bort, supra note 57; Zetter, supra note 57.

59. Peterson, supra note 57; Seal, supra note 57; Grisham, supra note 57; Betters, supra note 57; Ragan, supra note 57; Bort, supra note 57; Zetter, supra note 57.
followed through on the threat—they released the data and then erased and deleted Sony’s network.\footnote{Peterson, \textit{supra} note 57; Seal, \textit{supra} note 57; Grisham, \textit{supra} note 57; Betters, \textit{supra} note 57; Ragan, \textit{supra} note 57; Bort, \textit{supra} note 57; Zetter, \textit{supra} note 57.}

Almost immediately suspicion fell on North Korea. Sony was set to release “The Interview,” a comedy in which James Franco and Seth Rogan operate a television news program that is invited to interview North Korea’s leader, Kim Jung-Un, only to be asked by the Central Intelligence Agency to assassinate Kim.\footnote{The Interview (ColumbiaPictures, 2014); Peterson, \textit{supra} note 57; Seal, \textit{supra} note 57; Grisham, \textit{supra} note 57; Betters, \textit{supra} note 57; Ragan, \textit{supra} note 57; Bort, \textit{supra} note 57; Zetter, \textit{supra} note 57.} Understandably, North Korea was upset about this plot and had asked both the U.S. Government and the United Nations to prevent the release.\footnote{Ben Beaumont-Thomas, \textit{North Korea Complaints to UN About Seth Rogen Comedy The Interview, The Guardian} (July 10, 2014), http://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco.} When those requests failed, the thinking went, North Korea took action into its own hands.\footnote{David Gilbert, \textit{FBI Claim that North Korea Hacked Sony Pictures Bolstered by NSA Evidence, Int’l Bus. Times} (Feb. 20, 2015), http://www.ibtimes.co.uk/fbi-claim-that-north-korea-hacked-sony-pictures-bolstered-by-nsa-evidence-1488783} And it worked! After “The Interview” premiered in Los Angeles, the Guardians of Peace released a statement on December 16, specifically targeting “The Interview”:

\begin{quote}
Warning. We will clearly show it to you at the very time and places “The Interview” be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to. Soon all the world will see what an awful movie Sony Pictures Entertainment has made. The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time. (If your house is nearby, you’d better leave.) Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment. All the world will denounce the SONY.\footnote{See, \textit{e.g.}, Seal, \textit{supra} note 57.}
\end{quote}

Although the Department of Homeland Security represented that it was aware of no credible threats of this nature, Sony complied, halting the national release of “The Interview.”\footnote{Grisham, \textit{supra} note 57.} The reaction was swift and negative. President Obama said Sony had made a “mistake,” a sentiment echoed by

\begin{itemize}
\item\footnote{Peterson, \textit{supra} note 57; Seal, \textit{supra} note 57; Grisham, \textit{supra} note 57; Betters, \textit{supra} note 57; Ragan, \textit{supra} note 57; Bort, \textit{supra} note 57; Zetter, \textit{supra} note 57.}
\item\footnote{The Interview (Columbia Pictures, 2014); Peterson, \textit{supra} note 57; Seal, \textit{supra} note 57; Grisham, \textit{supra} note 57; Betters, \textit{supra} note 57; Ragan, \textit{supra} note 57; Bort, \textit{supra} note 57; Zetter, \textit{supra} note 57.}
\item\footnote{See, \textit{e.g.}, Seal, \textit{supra} note 57.}
\item\footnote{Grisham, \textit{supra} note 57.}
\end{itemize}
free speech advocates. The lone corner of praise for the decision came from North Korea. Although denying any involvement, North Korean state television had called the hack a “righteous deed.” The FBI had been on the case for weeks and, on December 19th, 2014, publicly attributed the attack on Sony to North Korean actors. The FBI based its conclusion on a technical analysis of the deletion malware, the “significant overlap” with previous malicious cyber activity linked to North Korea, and the “similarities” between the tools used against Sony and attacks North Korea had conducted against South Korean banks. Sony reversed course and set “The Interview” for limited Christmas Day release. The world rejoiced.

Briefly, seeing “The Interview” was a political act; “The Interview” earned about $36 million in initial release (although it cost about $77 million to make). The larger fallout for Sony, however, was still to come. Sony settled a lawsuit with the employees whose information was hacked for an estimated $8 million. Additional lawsuits are pending. Sony estimated its

66. Evan Perez et al., Obama: Sony ‘Made a Mistake’, CNN (Dec. 19, 2014), http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/ (“We cannot have a society in which some dictators someplace can start imposing censorship here in the United States because if somebody is able to intimidate us out of releasing a satirical movie, imagine what they start doing once they see a documentary that they don’t like or news reports they don’t like.”).


68. Id.

69. See David Gilbert, supra note 63.


71. This amount includes a record $31 million in video-on-demand sales (surely inflated by the controversy); however, the box office estimates were at just a $5 million gross (surely deflated by the limited release). See, e.g., Ryan Faughnher, ‘The Interview’ Earns $31 Million from VOD, $5 Million at Box Office, L.A. TIMES (Jan. 6, 2015), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sonys-the-interview-vod-box-office-20150106-story.html.

damaged IT infrastructure will cost $35 million to rebuild. Lost intellectual property only adds to the cost. In all, the damage is surely in the hundreds of millions of dollars.

But for the purposes of this article, the attack was (1) unlawful and disruptive, if not “violent” in the physical sense; (2) clearly intended to influence Sony and the general public against “The Interview”; (3) perpetrated by a minority group (in the sense that North Korea is on the outside of the civil world community) seeking imposition of its will against the majority; (4) motivated by a political and social ideology; (5) attributed to North Korean actors of indeterminate position; and (6) principally inflicted in the cyber world, but had real world monetary and hardware consequences, as well as real world damages to the Sony employees. This is what cyberterrorism looks like.

IV. THE BUREAUCRATIC ART OF CALLING IT LIKE IT IS

Seeking to not just play whack-a-mole with individual terrorists and terrorist groups, but rather to take a comprehensive approach of cutting off terrorists’ support networks, the U.S. Government has a system for designating “State sponsors of terrorism” and imposing sanctions upon such States to persuade them to abandon these pursuits.

Because nothing with this topic is ever clear-cut, there are actually three sources of law by which the United States may designate a foreign state as a
North Korea – State Sponsor of CyberTerrorism?

sponsor of terrorism: the Foreign Assistance Act of 1961; the Arms Control Export Act; and the Export Administration Act of 1979. Each of these acts have been amended many times since their enactment, so much so that not one of them even included “anything that would constitute construction of a list” of State sponsors in the initial iteration. As further evidence that “State sponsor” designation is somewhat ad hoc, the Export Administration Act of 1979 has technically expired, but has been sustained through Executive action.

Finally, although the three sources use a common standard—that the U.S. Government may designate a State as a sponsor of terrorism if it has “repeatedly provided support to international terrorism”—not one of the sources define the central term “international terrorism.” Two of the sources offer some color commentary or examples of representative acts that could constitute “international terrorism.” The Arms Export Control Act references that the term includes activities that:

[W]illfully aid or abet the international proliferation of nuclear explosive devices to individuals or groups, willfully aid or abet an individual or group in acquiring unsafeguarded special nuclear material, or willingly aid or abet the efforts of an individual or group to use, develop, produce, stockpile, or otherwise acquire chemical, biological, or radiological weapons.

Likewise, the Export Administration Act offers that the standard to determine whether one “repeatedly provide[s] support for acts of international terrorism” includes “the recurring use of any part of the territory of the country as a sanctuary for terrorists or terrorist organizations.”

Perhaps the most direct reference to a definition of terrorism comes from a related cross-reference. Congress requires an annual report on foreign countries that support international terrorism, which includes a discussion of designating them as a State sponsor of terrorism. What is the basis for this report, and thus the determining factor of the definition of “terrorism”? The Foreign Relations Authorization Act for Fiscal Years 1988 and 1989, which use the earlier discussed definition of terrorism to mean “premeditated, polit-

77. RENNACK, supra note 76, at 2.
78. Id. at 5.
79. Authority is maintained by the National Emergencies Act and the International Emergency Economic Powers Act, implemented through Executive Orders, most recently E.O. 13,222 of August 17, 2001. Id. at 2.
80. Id. at 2–3.
81. 22 U.S.C. § 2780(d) (2012); id. at 3.
82. RENNACK, supra note 76, at 3.
ically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.84

The point is that designation of a State as a sponsor of terrorism is more art than science; more politics than law. Designations are “determined” by the Secretary of State, but it is a whole-of-government process.85 For all of the ambiguity in the designation of State sponsors of terrorism, what is clear once a designation is announced are the ramifications directed upon the designated States. A designated State is limited or prohibited from many types of U.S. aid, or trade in, a designated state.86 Specifically, under the amended Export Administration Act of 1979, the Secretary of State may limit the public and private export of technology or goods, including defense articles, to designated States for national security or foreign policy reasons.87 Additionally, the amended Foreign Assistance Act of 1961 requires the United States to oppose any financial assistance to designated States given by international financial institutions, such as the World Bank, the Export-Import Bank, and the International Monetary Fund.88 To show it is serious, the United States even prohibits Peace Corp volunteers from serving in designated States and the United States denies the bounty of tax-free shopping to citizens of designated States.89

To again seek clarity from examples, the official list of States designated sponsors of terrorism has existed since 1979. Eight States have appeared on the list,90 but only three are now included: Syria, Iran, and Sudan.91 Syria, the only remaining charter member, is a known supporter of Hamas, has historically carried out numerous bombing campaigns abroad and domestically, and had conducted politically motivated assassinations.92 And that is all before the recent ruthless suppression of rebellion and the use of chemical weapons within its own territory, against their own citizens.93

Iran has been on the list since 1984, somehow avoiding listing during the hostage crisis. The Iranian Revolutionary Guards Corp both supports and

84. Id.
86. RENNACK, supra note 76, at 2.
87. Id.
88. Id.
89. Id.
90. Id. at 7 (discussing Syria, Iran, and Sudan as current members; Cuba and North Korea as recently removed members, and Libya (1979–2006), South Yemen (1979–1990), and Iraq (1979–1982 and 1990–2003) as previously removed members).
91. COUNTRY REPORT ON TERRORISM 2013, supra note 76.
92. Id. at 287–88.
93. Id. at 288.
North Korea
State Sponsor of CyberTerrorism?

commits acts of terrorism. Iran is a major supporter of Hizbollah (aka Hezbollah), has harbored known al Qaeda suspects, and has sought to develop both chemical and nuclear weapons, as well as proliferated technology thereof.

Probably the most interesting current inclusion as a State sponsor of terrorism is Sudan, which is described in the Department of State’s annual report as being a “generally cooperative partner of the United States on counterterrorism.” However, because Sudan allows both al Qaeda and the Lord’s Resistance Army to live and operate within its borders, it has been designated as a State sponsor of terrorism. Again, art, not science.

Also of interest, neither Afghanistan nor Pakistan has ever been designated a State sponsor of terrorism, despite the presence of the Taliban and al Qaeda in the former, and the admission, by former President Asif Ali Zadari, that Pakistan had deliberately “created and nurtured” terrorist groups as a matter of State policy.

Finally, it is instructive to look at the two States that were most recently removed from the list. Within the last year, Cuba was removed from the list. Cuba was added to the list in 1982 and remained until 2015 despite a lack of any recent evidence of support for terrorism (and an open acknowledgement of that fact). But political realities required Cuba remain on the list, until, suddenly, the realities no longer required the State’s inclusion, and Cuba was removed from the list as part of an initial normalization of relations.

The State removed most recently prior to Cuba was North Korea. Just six years after being identified in President Bush’s 2002 State of the Union address as a member of the “axis of evil,” the political tide turned and

94. Id. at 285.
95. Id.
96. Id. at 286.
99. See Sullivan, supra note 76.
100. Id.
101. Id.
102. Id.
global expediency, again, required the removal of North Korea from the State sponsors list. This removal was a condition for the “Six Party Talks” that sought resolution of North Korea’s weapons of mass destruction (WMD) program.

However, North Korea had initially and continually been designated a State sponsor per a rather convincing case. Prior to North Korea’s removal from the list, in considering legislative action against North Korea, the U.S. Senate had compiled a rather damming list of practices North Korea would have to address, including “weapons proliferation, harboring terrorists, counterfeiting U.S. currency, trafficking in narcotics, abduction of citizens of Japan and South Korea, and resolution of outstanding South Korean prisoner-of-war questions remaining from the 1950s conflict.” Even this summary omits earlier actions of North Korea to conduct or support terrorism, including the in-flight bombing of Korean Air Flight 858 in 1987 that killed 115 passengers (the principal event that caused North Korea to be added to the list in 1987).

Since the 2008 removal from the State sponsors list, North Korea has been implicated in additional activities counter to peace and order, including the:

- March 2010 sinking of the Cheonan, a South Korean naval vessel, killing forty-six sailors;
- November 2010 shelling of Yeonpyeong Island, killing two South Koreans and wounding eighteen more;
- weapons and material proliferation activities directed toward Iran, Syria, and Libya;

105. See Manyin et al., supra note 103, at 4.
106. Id.
107. Rennack, supra note 76, at 7; id. (Senator Sam Brownback said “A resolution expressing the sense of the Senate that certain benchmarks must be met before certain restrictions against the Government of North Korea are lifted, and that the United States Government should not provide any financial assistance to North Korea until the Secretary of State makes certain certifications regarding the submission of applications for refugee status.”).
108. Manyin et al., supra note 103, at 4.
111. See Paul K. Kerr et al., Cong. Research Serv., R43480, Iran-North Korea-Syria Ballistic Missile and Nuclear Cooperation, 1, 4, 6–8 (2015).
North Korea – State Sponsor of CyberTerrorism?

- ties to Hizbollah and Hammas, including providing weapons and logistics support;¹¹²
- continuing kidnappings and assassinations of North Korean refugees, critics, and foreigners abroad;¹¹³ and
- continuing development of WMD programs, including a submarine-launched ballistic missile capability¹¹⁴ and possible preparations for a fourth nuclear bomb test.¹¹⁵

Although some of these acts could be classified as acts of war and not terrorism, North Korea still seems to be involved with more than enough terroristic acts and actors to be listed on the State sponsors of terrorism list, even before considering the Sony hack.

V. I (TRY TO) KNOW WHO YOU ARE, BUT WHAT AM I?

So we come to the main idea of this article, that the Secretary of State must return North Korea to the U.S. State sponsors of terrorism list, and the designation should be explicitly and centrally tied to North Korea’s hack into Sony.¹¹⁶ The hack clearly falls within the definitions of terrorism under U.S. law, specifically as codified at 22 U.S.C. 2565f, the standard for designations to the State sponsors list.¹¹⁷


¹¹⁶. Such designation would explicitly and centrally rely on the Sony hack but, obviously, would also reference the many other acts of terrorism that North Korea has supported. But see Micah Zenko, Sorry, But North Korea Isn't a State Sponsor of Terrorism, FOREIGN POLICY (Dec. 22, 2014), http://foreignpolicy.com/2014/12/22/sorry-but-north-korea-isnt-a-state-sponsor-of-terrorism-cuba-unacceptables-list.

¹¹⁷. 22 U.S.C. § 2656f(d)(2); see generally MANYIN ET AL., supra note 103; RENNACK, supra note 76; David Auerbach, The Sony Hackers are Terrorists, SLATE (Dec. 17, 2014), http://www.slate.com/articles/technology/bitwise/2014/12/sony_pictures_hack_why_its_perpetrators_should_be_called_cyberterrorists
Perhaps hardline deniers of “cyberterrorism” would reject the idea that the Sony hack resulted in real-world damage, harkening back to traditional notions that someone must die or something must explode to constitute true terrorism. Again, of course, there is an inherent fundamental difference between the loss of intellectual property or privacy interests and loss of human lives. But the majority of terrorist acts directly impact only a limited number of people; the “terroristic” effect is, in many cases, caused by generating sympathy for the victims and fear of the seemingly random imposition of violence.

However, limiting the scope of terrorism to only those acts with real world damage negates two major points that demonstrate the “terroristic” effects of cyberterrorism. First, such a limitation denies modern reality, where real, monetary damage can be affected through simple manipulation of ones and zeros as surely as through placement of explosives. Second, cyberterrorism, as with all things cyber, greatly increases both the velocity and the scope of possible damage. We are all digitally connected and, thus, all targets can and could be attacked at the same time. Most fundamentally, the real world example of Sony’s decision to withdraw release of “The Interview,” even if temporarily, demonstrates cyberterrorists may still achieve their goals without causing real-world harm. It is time to start drawing lines as to what is, and is not, acceptable State practice in cyberspace.

Some might astutely point out that the impact of a designation of North Korea would be minimal, as they are already subject to major sanctions and restrictions through other sources of law, such as implementation of United Nations resolutions against North Korea. However, the 2008 removal from the State sponsors list did not bring an opening of relations or trade between the United States and North Korea; then, as now, the restrictions were in place for reasons that removing State sponsorship did not negate. No, in 2008, as it would again now, the principal reason for the designation is the negative political effect of affirmatively labeling North Korea a terrorist state.

North Korea has proven to be intensely aware of its geopolitical reputation. Indeed, removal from the State sponsors list was a diplomatic and polit-
ical victory for North Korea.121 Even within the police state of North Korea, where the government controls access to the media, a new designation as a State sponsor could have profound political impact on the regime, domestically and internationally.

Another concrete benefit of designation, not yet herein discussed, is that it nullifies provisions of the Foreign Sovereign Immunities Act122 such that the designated State is subject to the jurisdiction of U.S. court system and private actions brought therein.123 The principle of foreign sovereign immunity has existed in the United States for more than 200 years.124 Since its codification in 1976, foreign sovereign immunity has been invoked to attempt to quash a number of high-profile litigation efforts, such as those brought by survivors of the 9/11 attacks and victims of abuse by Catholic clerics.125 In cases where the defendants are fully stripped of immunity and the litigation proceeds to verdict, the monetary awards can be sizeable: $8 million for survivors and family of victims of the U.S.S. Cole bombing;126 a settlement of up to $10 million per family for the 259 victims of the Pan Am Flight 103 bombing;127 $300 million for families of an assassinated rabbi;128 and $300 million for kidnappings of American citizens.129 Obviously, not all

filed suits make it to judgment, and an even smaller percentage of judgments awarded are actually collected. But, as in the case with Libya and the Pan Am 103 bombing, settlement of such claims can be a concrete step toward reestablishing normalized relationships with the world community.\(^{130}\)

The Sony hack has already resulted in at least one class action lawsuit by the employees of Sony.\(^{131}\) While Sony settled the suit, it would, without a doubt, be interested in pursuing legal recourse against North Korea as the party ultimately responsible for the problem.\(^{132}\) Of course, it is unclear if Sony would prevail in court and unlikely that North Korea would appear and much less likely they would ever be made to pay an adverse judgment. But it would, if successful, be on the books as an issue needing resolution, should relations between the United States and North Korea ever improve.

It is important not to underestimate the value of this provision of the State sponsor designation process. Because data breaches are rarely criminally prosecuted, the majority of litigation is in a civil context to recover damages, by the affected parties. These suits easily reach the tens of millions of dollars.\(^{133}\) Where such suit could be based on an act of terrorism supported by a foreign State, one has to imagine that the damaged U.S. company would love to divert costs toward the designated State.

As stated, this is a proposal in favor of making something of “cyberterrorism,” and not an effort to categorically define the phenomenon or prove that it exists. And a move to designate States as sponsors of terrorism based upon or reliant upon cyber activity would not be without its problems. The great white whale of cyber response continues to be attribution. While a central point of terrorism is the perpetrator’s desire to link the act to his message, the point of designating State sponsors is that the sponsorship model allows the State to see a terroristic goal accomplished while the State is able to maintain plausible deniability of involvement. The FBI was quick and conclusive in blaming North Korean actors for the Sony hack, however, not all parties were convinced.\(^{134}\) One could imagine that with either a more sophis-
ticated attack or actor, the breadcrumbs might be even harder to identify and conclusively ascribe to a specific foreign State.

Alternatively, States that would proceed with terrorism may already be subject to enough restrictions (like North Korea) such that designation might be ineffective. First, the sanctions and restrictions that accompany State sponsor designation may be effectively redundant in application to a State, due to previous sanctions or restrictions. Second, a State may not be affected by “soft power” measures such as global perception or the risk of jurisdiction to U.S. legal judgments. As a result, designation would be a largely toothless measure, at very least in the sense that it is rarely a predicate consideration to more direct or military intervention.

Designation as a State sponsor could even provoke a further undesirable response. As mentioned, North Korean leaders have demonstrated that they can be thin-skinned when it comes to world opinion. But they also possess a nuclear bomb. Recent chatter in the U.S. political sphere about re-designation of North Korea as a State sponsor has led North Korea to deny allegations of its support for terrorism but also to “bolster its nuclear deterrent at a speed baffling to the imagination of the U.S.” in response. It would seem circular that calling a State a terrorist supporter would induce that State to support terrorism, especially since their support of terrorism places these States are on the list in the first place.

Finally, a great concern in leading the development of law, especially international law, is reciprocity. Any U.S. pronouncements for propriety in cyberspace could be used against the United States in the future. If North Korea were to be designated a State sponsor reliant on the Sony hack, how would the United States apply the principal to other States that are equally, or more, engaged in activities that could be considered to be cyberterrorism? Is today’s North Korea, tomorrow’s China, Russia, Israel, or even the United States? These scenarios would pose tricky political calculus for the United States between protecting the interests of both U.S. citizens and companies while also preserving diplomatic ties with allies and global powers.

In conclusion, the Sony hack—disastrous as it was for the company and its employees—offers a chance for the United States to make headway in establishing norms for unacceptable State behavior in cyberspace. Not all problems can be checked by a strongly worded rebuke, but not all problems


will warrant a military response. The existing process for designating a State as a sponsor of terrorism, if justified in this case explicitly upon North Korea's support for cyberterrorism, is a valid way for the United States to realize a geopolitical benefit, while also opening up the U.S. courts and possible financial benefit to aggrieved parties, all with very little cost or downside.