Overcoming Immunity Of Foreign Gov't Cyberattack Sponsors

By Jerry Goldman and Bruce Strong (December 2, 2020)

Jerry Goldman

Bruce Strong

State-sponsored cyberattacks endanger U.S. citizens and businesses, but U.S. litigants and courts have failed to think creatively in holding these sponsors liable. As the country relies more heavily on digital and cloud-based platforms to mitigate the spread of COVID-19, it is time for U.S. litigants and courts to chart a path for holding state actors liable for hacking.

In general, a foreign government is immune from lawsuits here in the U.S. — unless an exception to immunity, codified in the Foreign Sovereign Immunities Act, applies. When it comes to state-sponsored hacking, there are at least four relevant exceptions available under the FSIA to citizens and businesses to potentially hold foreign governments responsible for cyberattacks:

1. The noncommercial tort exception in Title 28 of the U.S. Code, Section 1605(a)(5);

2. The commercial activity exception in Section 1605(a)(2);

3. The justice against sponsors of terrorism exception in Section 1605B; and

4. The state sponsor exception in Section 1605A.

Litigants need to creatively argue for the application of these exceptions to combat a new and emerging threat to U.S. businesses and citizens: the threat of catastrophic cyberattacks.

The Noncommercial Tort Exception

The noncommercial tort exception provides that foreign governments are not immune from suit for cases:

> in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment.[1]

While several recent court cases have adopted an overly narrow, and, in our view, erroneous, interpretation of this exception,[2] the noncommercial tort exception remains a fruitful avenue to hold states liable for hacking.

For example, in Doe v. Federal Democratic Republic of Ethiopia,[3] the U.S. Court of Appeals for the District of Columbia Circuit dismissed the case against Ethiopia based upon the so-called entire tort rule. Under that judge-made rule, even if a foreign state intentionally directs harmful conduct toward the U.S., the foreign state is immune from suit if part of the tort occurred outside of the U.S.

But the D.C. Circuit did not sufficiently account for the plain language of Title 28 of the U.S. Code, Section 1605(a)(5), allowing suits against foreign governments to proceed where "damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States."

Nor did it sufficiently account for contrary authorities in the U.S. District Court for the District of Columbia case Letelier v. Republic of Chile and the U.S. Court of Appeals for the Ninth Circuit case Liu v. Republic of China,[4] in which foreign states were subject to suit in the U.S. even though their officials or employees did not act here. Letelier and Liu both involved official government conduct outside of the U.S., and, in both cases, the courts stripped immunity from the foreign government. Courts and litigants could apply this same line of reasoning to hold foreign governments accountable for directly targeting U.S. interests from abroad.

Further, courts applying the so-called entire tort rule do so through an erroneous reading of the one U.S. Supreme Court decision analyzing the noncommercial tort exception, Argentine Republic v. Amerada Hess Shipping Corp.[5] In that case, the Supreme Court refused to strip immunity from Argentina when it tortuously bombed the oil tanker Hercules in international waters about 5,000 miles from the U.S.

The court began its analysis as follows: "Section 1605(a)(5) is limited ... to those cases in which the damage to or loss of property occurs in the United States."[6] The ultimate holding of the case was not that the entire tort had to occur in the U.S., but rather that the damage had to occur in the U.S. At no time did the court discuss the location of the tortious conduct of the Argentine state actors — it only discussed the location of the damaged tanker.

The court ultimately held that "[b]ecause respondents' injury unquestionably occurred well outside the 3–mile limit then in effect for the territorial waters of the United States, the exception for noncommercial torts cannot apply."[7] This holding strongly implies that if the boat had been damaged within the territorial waters of the U.S., i.e., within the U.S., then the exception would have applied, without regard for where the Argentine bombers were located.

Any cyberattack victim attempting to strip immunity from a foreign government under the noncommercial tort exception should ensure that the court take a close look at Amerada Hess, because many courts have erroneously interpreted that decision to narrow the immunity exception, when it did no such thing. Like a bomber, a cyberattacker can most certainly strike a target from afar.

U.S. litigants seeking damages for cyberattacks should carefully analyze this case and its progeny in arguing for the application of the noncommercial tort exception to state-sponsored hacking that causes injury or damage in the U.S. State-sponsored attacks originating from abroad that cause damage to computer systems in the U.S. should fall within the noncommercial tort exception to immunity.

The Commercial Activity Exception

The commercial activity exception provides another possible avenue for many litigants targeted by foreign government cyberattacks. Under this exception, a foreign government is not immune from suit for a hack that involves commercial activity, where the hack has a connection with commercial activity and causes a direct effect in the U.S.[8] In Azima v. Rak Investment Authority, RAKIA, an organ of the United Arab Emirates, allegedly hacked

Azima's computer to gain an advantage in a negotiation with RAKIA's former CEO in which Azima was serving as a mediator.

The D.C. Circuit found that Azima and RAKIA engaged in ongoing commercial activity with each other, including various joint ventures and an agreement of sorts to assist in resolving a mediation between RAKIA and its former CEO. The court also found that RAKIA's alleged hack was in connection with this business activity, finding that the timing of the hack and the use of the information obtained from the hack to influence these business relationships suggested a "direct line between the hacking and the parties' commercial dealings." Finally, the court found a direct effect in the U.S. because nontrivial cognizable injury to Azima occurred in the U.S.[9]

The D.C. district court's analysis provides a path for a class of cyberattack victims to sue foreign governments in U.S. courts for any resulting injuries if they can demonstrate some connection between the cyberattack in question and commercial activity engaged in by the foreign government. The greater the connection U.S. litigants can demonstrate between a hack and ongoing commercial activity that lead to the attack, the more likely a court will apply the commercial activity exception.

Litigants need to be mindful of this option, especially given the D.C. Circuit's apparently narrow reading of the noncommercial tort exception. For example, if state sponsored hackers infiltrated a U.S. company's network to steal trade secrets for the purpose of giving their own companies a competitive commercial advantage or sponsored a cyberattack to influence ongoing business relationships between the state and the company, either of these cases could neatly fall under the commercial activity exception.

The Justice Against Sponsors of Terrorism Exception

Another compelling option U.S. cyberattack victims should consider is the Justice Against Sponsors of Terrorism Act, or JASTA, exception.[10] This exception strips immunity in cases where:

> damages are sought ... for physical injury to person or property or death occurring in the United States and caused by an act of international terrorism in the United States; and a tortious act or acts of the foreign state, or of any official, employee, or agent of that foreign state, while acting within the scope of his or her office, employment, or agency, regardless where the tortious act or acts of the foreign state occurred.[11]

In a typical hacking case, victims are seeking damages for physical injury to their property, i.e., damage to their computer or network. And, in some cases, victims are seeking damages for physical injury or death, such as when a hack targets hospitals or health systems, or the computer systems of cars, trains or airplanes while in transit. These damages necessarily are caused by the complained of cyberterrorist attack, tortuously committed by an agent of a foreign government, acting at the direction of the foreign government.

Two issues have yet to be litigated in the JASTA context. The first is whether damage to a computer or a network constitutes physical damage. In other contexts, courts have consistently accepted that damage to a computer system is physical damage.[12]

The second issue is whether cyberterrorism targeting U.S.-based computer systems and

networks is an act of international terrorism in the U.S. International terrorism under the Antiterrorism Act, Title 18 of the U.S. Code, Section 2331, includes criminal activities that:

> (A) involve violent acts or acts dangerous to human life;
>
> (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
> > (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.

Some cyberattacks are indeed potentially dangerous to human life; for example, the reported attack in early November by Russian-based hackers on a hospital network.

Depending on context, a court may find that wide-ranging hacking campaigns could be "intended to intimidate or coerce" U.S. citizens or our government. Similarly, a court could find that hacking occurs outside of the U.S., if it is initiated in Russia or transcends national boundaries, as the hackers are using malicious code that can be transmitted across the globe without regard to national borders in a matter of seconds and cause debilitating damage to U.S.-based computer systems.

To our knowledge, no court has yet applied the JASTA exception to acts of cyberterrorism. That is because no litigant, to our knowledge, has argued for its application. But one could envision a strong argument against immunity when foreign state actors conduct cyberattacks on U.S. electrical grids, schools, refineries and pipelines, public transportation systems or dams and power plants. Litigants need to be aggressive and creative in pursuing cases against those that sponsor hacking campaigns, or those campaigns will continue to proliferate, crippling more and more U.S. businesses.

The State Sponsor Exception

Finally, against certain designated state sponsors of terrorism — currently Iran, Syria, Sudan and North Korea — the state sponsor exception,[13] may be available to U.S. litigants. The immunity analysis is very similar to the JASTA exception, but instead of requiring an act of international terrorism, the state sponsor exception applies to acts of "torture, extrajudicial killing, aircraft sabotage, hostage taking, or the provision of material support or resources for such" acts.

While this definition does not at first blush appear to apply to hacking, it might, depending on what is hacked. If an airplane or air traffic control is hacked, that would likely constitute aircraft sabotage. If a hospital or other healthcare network were hacked resulting in patients dying due to lack of access to medical care, a court may find that this constitutes extrajudicial killing, and if a hack targets infrastructure that traps people in a particular location, that could constitute hostage-taking.

More commonly, a typical ransomware attack, in which hackers lock out the target's computer system until the target pays a ransom, could constitute hostage-taking within the

meaning of the state sponsor exception.

While U.S. litigants and courts have been slow to date to respond effectively to acts of cyberterrorism, a cyberattack against U.S. interests could easily fall into any one of these four exceptions to immunity. In an age in which businesses increasingly rely on cloud-based and digital platforms to mitigate the spread of COVID-19, U.S. litigants need to utilize — and courts need to recognize — these four immunity exceptions to protect our computer networks and valuable data from foreign attacks.

Jerry S. Goldman is a shareholder and Bruce Strong is an attorney at Anderson Kill PC.

[1] 28 U.S.C. § 1605(a)(5).

[2] See Doe v. Fed. Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017); Democratic Nat'l Comm. v. Russian Fed'n, 392 F. Supp. 3d 410 (S.D.N.Y. 2019); Broidy Capital Mgmt., and LLC v. Qatar, No. CV 18-2421-JFW(EX), 2018 WL 6074570 (C.D. Cal. Aug. 8, 2018).

[3] Doe v. Fed. Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017).

[4] Letelier v. Republic of Chile, 488 F. Supp. 665 (D.D.C. 1980); Liu v. Republic of China, 892 F.2d 1419 (9th Cir. 1989).

[5] 488 U.S. 428 (1989). A number of courts and commentators we suggest misapply the holding of Amerada Hess. Repeat a mantra long enough, and it can become "law" even if it is contrary to Supreme Court precedent.

[6] Id. at 439.

[7] Id. at 441.

[8] See Azima v. RAK Inv. Auth., 305 F. Supp. 3d 149 (D.D.C. 2018).

[9] The D.C. Circuit ultimately reversed the district court on entirely different grounds finding that a forum selection clause in a contract required litigation in England, but even then, the D.C. Circuit only dismissed the case once it received assurances from RAKIA that it would waive any immunity defense in English court. Azima v. RAK Inv. Auth., 926 F.3d 870 (D.C. Cir. 2019).

[10] 28 U.S.C. § 1605B.

[11] Id.; see also Anti-Terrorism Act ("ATA"), 18 U.S.C. § 2331.

[12] See, e.g., Lambrecht & Assocs., Inc. v. State Farm Lloyds, 119 S.W.3d 16 (Tex. App. 2003); NMS Servs. Inc. v. The Hartford, 62 F. App'x. 511 (4th Cir. 2003); Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co., 435 F. Supp. 3d 679 (D. Md.

2020); Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-cv-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000).

[13] 28 U.S.C. § 1605A.