AMERICANBARASSOCIATION
Forum on the Entertainment & Sports Industries

VOLUME 35, NUMBER 2
FALL 2019

ENTERTAINMENT AND SPORTS LAWYER

A PUBLICATION OF THE AMERICAN BAR ASSOCIATION FORUM ON THE ENTERTAINMENT & SPORTS INDUSTRIES

Chair's Column

Dear Forum Members,

This is my first message to you as the incoming Chair of the Forum. I look forward to seeing you all at the Forum's Annual Meeting at the Four Seasons Hotel in Las Vegas, October 11, 12 and 13.

We have an exciting program of panels on cutting edge issues including a Mock Negotiation on eSports Investment and Team Ownership; Legal Issues in Protecting a Client's Brand; a Fireside Chat with Seth Krauss, Chief Legal Officer of Endeavor; Mindfulness; Sports Gambling; a Digital Platforms roundtable; a Plenary with leading next GEN Entertainment and Sports Lawyers; and a Keynote Address by Merck Mercuriadis, CEO and Founder of Hipgnosis Songs Ltd.


Peter J. Strand

In addition, there will be great networking opportunities including a Nightcap Reception on Friday night, a conference wide luncheon on Saturday, the annual Ted Reid reception on Saturday night and several offsite Behind the Scenes activities.

This year the Forum instituted new CLE programming to coincide with our Spring Governing Committee meeting. In April, we met at the Guest House at Graceland in Memphis, Tennessee and presented a half-day CLE program at the Cecil C. Humphreys School of Law at the University of Memphis. This programming will continue in April 2020 when the Governing Committee meets in Milwaukee, Wisconsin next year.

I look forward to seeing you all in Vegas. ■

Best regards,

Peter J. Strand
Chair, ABA Forum on the Entertainment & Sports Industries

IN THIS ISSUE

ENTERTAINMENT AND SPORTS LAWYER

Forum Information

Forum on the Entertainment & Sports Industries
American Bar Association
321 N. Clark St.
Chicago, IL 60654
Phone: 312-988-5658
Fax: 312-988-5677

AMERICANBARASSOCIATION

Forum on the Entertainment & Sports Industries

Table of Contents

Renewed for Another Season

International Cyberattacks on the Entertainment Industry

Lucas J. Tanglen and Reymond E. Yammine

Executives, in-house lawyers, and outside counsel might already be keenly aware of the continuous string of cyberattacks that have recently plagued entertainment companies. On the other hand, keeping track of the arcane dealings of United Nations (UN) committees is, quite understandably, probably not a very high priority for many of those same industry-savvy professionals. Nonetheless, these two subjects have converged in a manner that anyone involved in running or counseling an entertainment business may find deeply troubling. Specifically, the UN group charged with reaching a consensus on international norms governing conduct in cyberspace admitted failure in 2017, and despite some efforts to revive discussions in 2018, there is still no end in sight for the damaging cyberattacks carried out by foreign governments, militaries, and political actors that have adversely impacted companies in the entertainment field. Accordingly, it remains vitally important for entertainment companies to understand their potential vulnerability to nation-state cyberattacks and the possibility of using their insurance to manage those risks.

CYBER ATTACKS REPEATEDLY HIT ENTERTAINMENT BUSINESSES

A 2018 survey of cyber security decision-makers at U.S. media and entertainment companies concluded that 51% of such firms experienced *three or more* cyberattacks over a 12-month period.[1] In a 2015 survey of media executives, 46% reported being subject to cyberattacks in the prior year.[2] Respondents to the 2015 survey attributed those cyberattacks to a range of attackers, including "foreign nation-states."

There are many reasons why an entertainment company might be an attractive target for a cyberattack. For example, a TV production company might house valuable intellectual property—such as unaired episodes of popular shows—on its digital servers. Confidential e-mail discussions regarding high-profile projects, celebrities, or executives might be used to blackmail or embarrass businesses and individuals. Media companies with expansive online presences might simply present a cyber target that is too large to resist, particularly where they communicate with and deliver content to customers online, thereby potentially exposing a wealth of valuable customer data.

In one of the most notable entertainment cyberattacks—the 2017 attack on HBO—the value of the target's intellectual property contributed to the attack's effectiveness. As alleged by federal prosecutors, HBO's attacker successfully stole unaired episodes of several original HBO series, scripts and plot summaries for unaired programs (including *Game of Thrones*), confidential cast and crew contact lists, e-mails belonging to at least one HBO employee, and online credentials for HBO social media accounts.[3] According to prosecutors, this attack was neither random nor spontaneous. To the contrary, charging documents describe an "online reconnaissance" operation on HBO's networks and employees. The perpetrator allegedly succeeded in compromising not one, but multiple authorized user accounts. The suspect allegedly spent approximately three months stealing confidential and proprietary information. With the theft complete, the attacker allegedly commenced an "extortion scheme," demanding $6 million worth of Bitcoin from HBO based on a threat of releasing the stolen content.

As entertainment firms assess the likelihood of similar attacks occurring, at least two significant points from the HBO attack are worth noting. First, the government asserts that the alleged HBO attacker is an Iranian national who previously hacked computer systems for his country's military, raising the specter of foreign-government involvement in a targeted cyberattack on a US business. Second, despite his recent indictment by federal prosecutors, it is not clear that the alleged thief will ever face trial in the US, given the absence of an extradition treaty between the US and Iran. As such, the threat of criminal charges in the US may have limited deterrent effects on international cybercriminals.

There have been many other cyberattacks on entertainment and media targets, some of which have been publicly attributed to foreign nation-states or associated organizations. For example:

- In 2014, 21 of the world's 25 largest news outlets had been targeted by likely state-sponsored hacking attacks, according to findings presented by a pair of Google security engineers.[4]

- In 2015, the French television network TV5Monde was taken off the air by a malware attack whose perpetrators initially claimed to be associated with the Islamic State, but were later understood to be part of a group of Russian hackers who carry out attacks that are perceived to advance Russia's interests. The attack used highly targeted (bespoke) malicious software designed to destroy the network's systems, and it succeeded at knocking all twelve of the network's channels off the air for several hours. A network executive said that fast action by a technician who fortuitously was onsite during the attack saved the company from "total destruction." An investigation revealed that the attackers had carried out reconnaissance to understand how TV5Monde broadcast its signals, and they had used seven different points of entry to carry out the attack.[5]

- A hacker (or hackers) breached an audio post-production studio's network in late 2017, resulting in the unauthorized leak of an episode of *Orange is the New Black*, according to media reports. Despite being paid about $50,000 in Bitcoin, the hacker reportedly leaked the episode to "punish" the studio for contacting the FBI.[6]

- Saudi Arabia's General Entertainment Authority, which sponsors concerts and shows in that nation, announced in September 2017 that its website had been hit by a cyberattack from outside the country.[7]

While it is clear that cyberattacks may be committed against entertainment companies for a variety of reasons (*e.g.*, for money, as a hoax, or for political reasons), it is also clear that entertainment companies exist in a cyber world in which nation-states are willing to use cyberattacks against diverse targets in order to advance geopolitical agendas. The President's National Infrastructure Advisory Council has stated: "Cyber is the sole arena where private companies are the front line of defense in a nation-state attack on US infrastructure."[8] The Council of Economic Advisers warns that nation-states may attack businesses "potentially as a retaliation against sanctions or other actions taken by the international community."[9] While recently describing the cyber threats that the US currently faces across many fronts, US Director of National Intelligence Dan Coats ominously compared the current situation to the indications of a possible terrorist attack in the lead-up to September 11, 2001: "The warning lights are blinking red again. Today, the digital infrastructure that serves this country is literally under attack."[10]

THE FAILURE OF UN TALKS ON INTERNATIONAL NORMS FOR CYBERSPACE

In the face of these threats, media companies would be justified in taking some small comfort from the prospects for an effective, international legal order that would punish and deter global cyberattacks. Unfortunately, recent events strongly suggest that this would be wishful thinking.

A decade's worth of international discussions regarding the future of international law in cyberspace came to a fruitless conclusion in 2017.[11] The UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security had been considering the application of international norms to the member countries' activities in cyberspace. The talks had the potential to resolve questions such as whether, and under what circumstances, a nation might be justified in responding to a foreign-government cyberattack with counter-cyberattacks or even military force. Traditional powers, including the United States, China, and Russia, had participated in the effort,[12] but negotiations were ultimately frustrated, as divisions along old "Cold War" lines prevented agreement on key terms.[13] Furthermore, although 2018 and early 2019 brought the creation of two new UN Groups: a 6th GGE[14] and an open-ended working group,[15] it is unclear whether either of these groups will be able to overcome the 2017 impasse. Indeed, the creation of these separate groups reflects the same ideological division that lead to the failure of the GGE in 2017.[16] One internet policy advocate stated: "[T]here are now two parallel work streams on this topic in [the UN General Assembly], with different procedures, led by governments with competing visions for how the UN should address norms on international security in cyberspace."[17]

This is important to US entertainment companies because recent history—including the cyberattacks on HBO and TV5Monde—shows that attacks by nation-states may have substantial adverse effects on those companies. Accordingly, entertainment companies need to understand their potential vulnerability to nation-state cyberattacks and the possibility of using their insurance to manage those risks. The remainder of this Article explores the development and ultimate collapse of the UN cyber talks and related insurance considerations for entertainment companies.

In 1999, the UN General Assembly recognized the "scientific and technological" value that cyberspace represented and the need to protect its civilian uses.[18] The General Assembly concluded that it was "necessary to prevent the misuse or exploitation of information resources" and that member states should work toward considering the "[a]dvisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality."[19]

The GGE officially began its work in 2004, and, over the years, has been seeking to promote cyber security and develop a framework to govern international conduct in cyberspace. The GGE recognized the impact that the development of information and communications technologies (ICTs) could have on matters of national security. In 2009, the group alerted member states that the growing use of ICTs would create "new vulnerabilities and opportunities for disruption."[20] In 2013, the GGE acknowledged the importance of maintaining an international legal framework that could preserve peace in cyberspace. The group's recommendations stated, "the application of norms derived from existing international law . . . is essential to reduce risks to international peace, security and stability."[21] Furthermore, "States must not use proxies to commit internationally wrongful acts" and should seek to ensure "that their territories are not used by non-State actors for unlawful use of ICTs."[22] In 2015, the GGE noted "[t]he diversity of malicious non-State actors, including criminal groups," which could create misperception of state action and the "possibility of harm to their citizens, property and economy."[23] The GGE called for increased cooperation between nations and the use of ICTs in a way consistent with preserving "global connectivity and the free and secure flow of information."[24]

Despite such indications of progress, 2017 brought the breakdown of the GGE's talks. The failure of the negotiations was driven, in part, by what media described as divisions along Cold War lines.[25] On one side, the US expert to the GGE, Michele Markoff, argued that the GGE was misguided in not seriously considering the inclusion of the member states' right to self-defense against foreign-state

attacks.[26] The right to self-defense, in its broad sense and as memorialized in Article 51 of the UN Charter, refers to a state's right to respond to an "armed attack" against it.[27] Markoff argued that the recognition of the right to self-defense in the cyber context would "help reduce the risk of conflict by creating stable expectations of how states may and may not respond to cyber incidents they face."[28] On the other side, Cuba opposed recognizing a right to self-defense, arguing that such a regime would "convert cyberspace into a theater of military operations and . . . legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs."[29]

This ideological division appears to be ongoing, with no end in sight. Following the UN Secretary's calls for action in light of "the permanent violation of cybersecurity" in early 2018,[30] the UN General Assembly approved two separate resolutions to attempt to revive the talks. The Russia-sponsored resolution called for a new open-ended working group and 13 "international rules."[31] The US-sponsored resolution called instead for the formation of a new GGE.[32] The division along Cold War lines arguably remained evident,[33] and although there continues to be international interest in managing global cyber threats, there is no indication that a meaningful solution is near or that the disagreements that doomed the talks in 2017 have gone away.

CYBER RISK MANAGEMENT AND INSURANCE CONSIDERATIONS

The potential losses to an entertainment company from a cyberattack are vast and varied. For example, if a malware attack against a television production studio destroys digital assets such as scripts, casting lists, and video clips, the costs of recreating the lost materials could be substantial. If a ransom attack compromises proprietary IP such as unaired episodes, the studio could incur loss in the form of payment of the ransom demand or the lost value of the IP in the event that it is leaked (or both, if the IP is leaked after payment). If networks or computers are rendered unusable in a cyberattack, the studio might incur "business interruption" losses in the form of payroll costs and lost profits during the downtime, as well as "extra expense" losses for the cost of taking any steps necessary to minimize the interruption. In the event of a breach of private data, an entertainment company might experience damage to its reputation and brand, various response costs in the form of fees for forensic investigators, notification of affected consumers or vendors, and establishment of call centers and credit monitoring.

Given the immense threat posed by international cyberattacks and the apparent failure of the international community to develop a legal framework to deter nation-state cyberattacks, there is no time like the present for policyholders to understand potential insurance coverage for these types of risks. "Traditional" insurance may provide coverage for certain cyber-related losses and liabilities. Such traditional coverages include commercial property policies, commercial general liability insurance, crime policies, and errors and omissions (or professional liability) insurance policies. Policyholders will want to review carefully whether any "cyber" exclusions that may limit or divest the policyholder of coverage have been included in those policies. Depending on policy wordings, insurers may assert that certain cyber risks are not covered by such traditional insurance.

In recent years, the number and variety of specialty cyber-insurance coverages has grown significantly, with approximately 70 insurers currently offering some form of cyber coverage. Cyber policies may differ widely in the types of coverages provided and the scope of coverage that would be provided in the event of a cyberattack. "Media liability" coverage—for losses related to defamation, privacy/publicity violations, copyright violations, and other liability risks related to the creation or dissemination of media content—is often included as a component of cyber insurance policies. In fact, given their line of business, some entertainment companies might have purchased a standalone media liability insurance policy, which may (or may not) include certain cyber coverages. Given the many forms in which cyber insurance is sold and the many distinct types of coverages that it might include, entertainment businesses might find it useful to review the types of cyber coverages that appear in their existing insurance.

For example, because of the nature of cyberattacks, "business interruption" coverages are likely to be implicated. With cyberattacks like WannaCry and NotPetya, a victim's entire computer network may become unusable for a sustained period of time. In the deadline-oriented world of the entertainment industry, such downtime may translate into significant costs, including lost profits and the extra expenses of mitigating such losses. Entertainment policyholders may wish to consider whether their current cyber policy contains coverage for business interruption and whether there are any relevant policy exclusions for attacks allegedly or actually initiated by nation-states.

We note that some insurance policies contain exclusions related to "war," "warlike action," "terrorism," "hostilities," and "hostile acts," which an insurer might invoke in an attempt to avoid coverage. Policyholders should not assume that such an exclusion necessarily bars coverage for a particular cyberattack. The precise wording of each exclusion, which may vary substantially among policies issued by different insurers, should be applied carefully and narrowly. For example, depending on the wording of the exclusion, it may be very difficult for an insurer to establish that a particular cyberattack rises to the level of, for example, "war" or "warlike action." Similarly, the undefined term "hostilities" (for example) is very vague and ambiguous. Where an ambiguous term like "hostilities" appears in a list with other excluded events such as "war" and "warlike action," the doctrine of *ejusdem generis* holds that the meaning of the ambiguous term should be restricted to something similar to "war" or "warlike action." Also, the origin of a cyberattack is often unclear and subject to dispute, even years after the attack occurred. It may be inappropriate for an insurer (who generally bears the burden of proving that an exclusion applies) to invoke an exclusion where there exists any uncertainty as to a cyber attack's origin, even if government

or media sources have attributed the attack to a government or military entity.

Most cyber policies also contain exclusions for property damage and bodily injury. Cyber-physical attacks are real, and are no longer just the product of speculation. For example, a cyberattack may affect equipment connected to the so-called "internet of things," such as remotely operated production cameras or on-premises security systems (*e.g.*, locks, gates, security cameras). A careful analysis of how property damage and bodily injury exclusions might apply may be very useful in assessing the responsiveness of a cyber policy to such a cyber-physical attack.

As the foregoing suggests, it is in an entertainment business's interest to carefully review, in consultation with insurance coverage counsel, the wording of any cyber insurance that the company currently has in effect or is considering purchasing. Policyholders and their counsel may be able to negotiate with insurers during the placement or renewal of an insurance program to obtain more favorable wording than the "off-the-shelf" language might provide (including with respect to "war" and other exclusions).

Likewise, in the event that an entertainment business finds itself in the unfortunate position of being a victim of a cyberattack, coverage counsel can assist with a prompt, careful review of any potentially applicable insurance policies and analyze the necessary steps to pursuing insurance coverage including the timely provision of notice to relevant insurers. ■

Lucas J. Tanglen is a senior associate in the Pittsburgh office of K&L Gates, LLP. He represents insurance policyholders in many industries, including entertainment and sports, with respect to a wide range of insurance-related matters including the review and placement of cyber insurance policies. He can be reached at lucas.tanglen@klgates.com.

Reymond E. Yammine is an associate in the Pittsburgh office of K&L Gates, with a broad-ranging, litigation-focused practice. He can be reached at reymond.yammine@klgates.com.

ENDNOTES

1. GlobeNewswire, *Over Half of Media and Entertainment Firms Experienced Three or More Cyber Attacks over a 12-Month Period, Reveals Hiscox Survey*, MarketWatch (Sept. 12, 2018), https://www.marketwatch.com/press-release/over-half-of-media-and-entertainment-firms-experienced-three-or-more-cyber-attacks-over-a-12-month-period-reveals-hiscox-survey-2018-09-12.

2. Marianne Zumberge, *Cyber Attacks on the Rise in Media Biz Since Sony Hack: Survey (Exclusive)*, Variety (Nov. 5, 2015), https://variety.com/2015/digital/news/sony-hack-anniversary-cybersecurity-data-1201633671/.

3. *Acting Manhattan U.S. Attorney Announces Charges Against Iranian National for Conducting Cyber Attack and $6 Million Extortion Scheme Against HBO*, Dept. of Justice (November 21, 2017), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting.

4. Jeremy Wagstaff, *Journalists, media under attack from hackers - Google researchers*, Reuters (Mar. 28, 2014), https://www.reuters.com/article/uk-media-cybercrime/journalists-media-under-attack-from-hackers-google-researchers-idUKBREA2R0ET20140328.

5. Gordon Corera, *How France's TV5 was almost destroyed by 'Russian hackers,'* BBC (Oct. 10, 2016), https://www.bbc.com/news/technology-37590375.

6. Janko Roettgers, *Hackers Confirm Leaking 'Orange Is the New Black' Despite Ransom Payment*, Variety (June 20, 2017), https://variety.com/2017/digital/news/dark-overlord-ransom-payment-confirmation-1202473108/.

7. *Saudi entertainment authority says hit by cyber attack*, Reuters (Sept. 29, 2017), https://www.reuters.com/article/us-saudi-cyber-attack/saudi-entertainment-authority-says-hit-by-cyber-attack-idUSKCN1C427R.

8. *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, Dept. of Homeland Sec. (August 2017), https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

9. *The Cost of Malicious Cyber Activity to the U.S. Economy*, White House (Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, at 3.

10. *Transcript: Dan Coats Warns The Lights Are 'Blinking Red' On Russian Cyberattacks*, NPR (July 18, 2018), https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks.

11. *See* Michele Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.S. Mission to the U.N. (June 23, 2017) (the "Markoff Remarks"), https://usun.state.gov/remarks/7880.

12. *See, e.g.*, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/65/201, at 5, (July 30, 2010) (the "2010 GGE Report").

13. *See* Owen Bowcott, *Dispute along cold war lines led to collapse of UN cyberwarfare talks*, The Guardian (Aug. 23, 2017), https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges.

14. G.A. Res. 73/266, Advancing responsible State behaviour in cyberspace in the context of international security (Jan. 2, 2019).

15. G.A. Res. 73/27, Developments in the field of information and telecommunications in the context of international security (Dec. 11, 2018).

16. *First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct*, U.N. (Nov. 8, 2018) ("U.N. Press Release Nov. 2018"), https://www.un.org/press/en/2018/gadis3619.doc.htm.

17. Deborah Brown, *UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online*, APC (Jan. 10, 2019), https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed.

18. G.A. Res. 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security (Jan. 4, 1999).

19. *Id.*

20. 2010 GGE Report, U.N. Doc. A/65/201, at 2.

21. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 2, U.N. Doc. A/68/98 (June 24, 2013).

22. *Id.* at 8.

23. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 6, U.N. Doc. A/70/174 (July 22, 2015).

24. *Id.* at 13.

25. *See* Bowcott, *supra* note 14.

26. *See* Markoff Remarks, *supra* note 12.

27. *See* U.N. Charter art. 51.

28. *See* Markoff Remarks, *supra* note 12.

29. Declaration by Miguel Rodriguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017), http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

30. U.N. Press Release Nov. 2018, *supra* note 17.

31. Developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/C.1/73/L.27/Rev.1 (Oct. 29, 2018).

32. Advancing responsible State behaviour in cyberspace in the context of international, U.N. Doc. A/C.1/73/L.37 (Oct. 18, 2018).

33. U.N. Press Release Nov. 2018, *supra* note 17.