SPACE HACKERS

The need for updates in national and international cybersecurity laws.

WRITTEN BY **GUILLERMO "WILL" S. TREVINO**

Law and sci-fi nerds unite. In comic book shops across America, mentioning one space opera (subgenre of science fiction that deals with space adventures) over another spurs debates as to whether Star Wars or Star Trek is the better sci-fi enterprise (pun intended for those Trekkers who caught that). *Star Wars: Episode IV—A New Hope* was released on May 25, 1977,[1] while the television series Star Trek debuted on September 8, 1966.[2] Yet, the internet as we know it today did not become available until the early 1990s.[3] Audiences then did not realize they were witnessing the first instances of failed cybersecurity as R2-D2 famously saved the protagonists of the movie franchise from the garbage smashers or when Captain Kirk was able to lower Khan's shields and take over his spaceship remotely in *Star Trek 2: The Wrath of Khan*.

Sci-fi is often credited for inspiring technology that we have today. And much like the fictional Galactic Empire or United Federation of Planets, governments on Earth, specifically within the United States, provide various services to the public, which often includes police, fire, water, sewer and electrical utilities, and mass transit services. Federal, state, and local governments are also in the business of data collection as they maintain the personal identifiable information of the customers who utilize these services.[4]

As an employer, these governmental bodies maintain confidential personnel information on their employees as well.[5] The federal government alone has approximately 4 million federal employees whose information was leaked from a cyberattack on the Federal Office of Personnel Management in June 2015.[6] This equates to approximately 25.7 million records.[7] Nationwide, it is estimated that more than 293 million records held by government agencies have been breached.[8] And each breach comes with a hefty price tag as data breaches are estimated to cost approximately $8.64 million, or an average of $146 per record, and these numbers are climbing.[9]

The data keep pouring in as government bodies are also one of the largest consumers, as these entities purchase various commodities and services that allow them to then provide the services to the public. In receiving responses to requests for proposals or bids, governmental bodies tend to house a wide array of proprietary and financial information belonging to third-party vendors that they deem confidential.[10] Many times, when a request for information is made under the Texas Public Information Act, the state's right to information laws, upon request for a ruling from a governmental body, the attorney general will issue a ruling that such confidential and proprietary information may be withheld from public disclosure.

Moreover, much of the nation's critical infrastructure systems that control traffic—airports, dispatch, water, sewer and electrical plants, and a wide range of vital infrastructure—is controlled by state and local governments. On February 5, 2021, residents of Oldsmar, Florida, learned what could happen to their water supply when a cybercriminal infiltrated the water treatment plant and started to increase lye, a dangerous and poisonous chemical that is comparable to drain cleaner.[11] More recently, the website of Bradley International Airport, in Windsor Locks, Connecticut, was attacked by cybercriminals who left a message related to the United States' supply of arms to Ukraine: "When the supply of weapons to Ukraine stops, attacks on the information structure of your country will instantly stop. America, no one is afraid of you."[12] These are just a few examples of how cybercriminals can threaten the public.

Confidential records and critical infrastructure systems maintained by governmental bodies are at risk of a breach from cybercriminals.[13] Quite simply put, they are easy targets. Yet, when it comes to expenditures on cybersecurity training or infrastructure, corporations far outpace governmental bodies.[14] Governments have seen an uptick in ransomware attacks.[15] Once a computer or system is infiltrated, cybercriminals seek ransom payment in exchange for the information they took—a form of modern-day blackmail.[16] Many cities have paid the ransom out of the taxpayers' coffers, while others have relied on cyber insurance to pay the ransom.[17] Legislation was introduced in the 87th Texas legislative regular session that would have prohibited cities, and other political subdivisions, from paying a ransom,[18] but it never made it out of committee.

Unfortunately, only 38% of federal and state government employees have been trained in cybersecurity.[19] And consider that 90% of new skills are generally lost after training.[20] These are clear recipes for disaster. Simply put, a cybersecurity breach is a manmade disaster.

But what about critical infrastructure in space? At the time of this writing, Ukraine is in the midst of defending against

an aggressor that has infiltrated the boundaries of its nation. Much of the success of the Ukraine defense has been information received from allies using geospatial intelligence from satellites orbiting the Earth.[21] Moreover, public-private partnership and laws such as the Spurring Private Aerospace Competitiveness and Entrepreneurship, or SPACE Act of 2015, have once again inspired a new space race as commercial companies such as SpaceX, Blue Origin, and Virgin Galactic are competing for the uncharted territory of space transit.

The Union of Concerned Scientists, a nonprofit organization founded by scientists and students at the Massachusetts Institute of Technology that advocates for a safer and healthier world, estimates that there are approximately 4,852 satellites orbiting Earth.[22] Of this number, the United States has 2,944 satellites with 85%, or 2,516, being commercial.[23] On February 25, 2022, the National Institute of Standards and Technology, or NIST, published draft Interagency/Internal Report 8270, or NISTIR 8270, that states: "Space is an emerging commercial critical infrastructure sector that is no longer the domain of only national government authorities.[24] Space is an inherently risky environment in which to operate, so cybersecurity risks involving commercial space—including those affecting commercial satellite vehicles—need to be understood and managed alongside other types of risks to ensure safe and successful operations."[25] This second rendition of NISTIR 8270 aims at providing a "specific method for applying the Cybersecurity Framework (CSF) to commercial space business and describes an abstracted set of cybersecurity outcomes, requirements, and suggested controls."[26]

Russia recently conducted an anti-satellite test and launched a missile at one of its old spy satellites hurling debris through space requiring the crew of the International Space Station to take shelter in a spacecraft.[27] Arguably, this act was not a violation of the Outer Space Treaty of 1967 since no nuclear weapon was used. But sending deadly debris into space like a scene from the 2013 film *Gravity* is the least of our worries.

Gen. David Thompson of the United States Space Force, a military service that serves to protect United States and allied interests in space and to provide space capabilities to the joint force,[28] was quoted in *The Washington Post*: "The threats are really growing and expanding every single day. And it's really an evolution of activity that's been happening for a long time. We're really at a point now where there's a whole host of ways that our space systems can be threatened."[29] But space has yet to be declared a critical infrastructure sector.[30] That may change as the U.S. House of Representatives introduced HR 3713—the Space Infrastructure Act—that would designate space systems, services, and technology as critical infrastructure.[31]

With the advent of World War II, which spanned from September 1, 1939, to September 2, 1945, international laws have made great strides with several treatises being entered into or ratified by members of the United Nations.[32] Collectively, these international laws define the legal responsibilities of states in their relations with each other, human rights, disarmament, international crime, environment and sustainable development, international waters, outer space, global communications, and world trade.[33] Worldwide, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, or simply the Outer Space Treaty, signed in 1967 through the United Nations and made official, or ratified, by 105 countries, governs the activities of spacefaring nations or states as used in the treaty.[34] The Outer Space Treaty provides that:

- the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries and shall be the province of all mankind;
- outer space shall be free for exploration and use by all States;
- outer space is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means;
- States shall not place nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies or station them in outer space in any other manner;
- the Moon and other celestial bodies shall be used exclusively for peaceful purposes;
- astronauts shall be regarded as the envoys of mankind;
- States shall be responsible for national space activities whether carried out by governmental or non-governmental entities;
- States shall be liable for damage caused by their space objects; and
- States shall avoid harmful contamination of space and celestial bodies.[35]

Shortly after the Outer Space Treaty was adopted, the United Nations created several other treaties related to space activities:

- Rescue Agreement (1968)
- Space Liability Convention (1972)
- Registration Convention (1976)
- Moon Treaty (1979).[36]

However, none of these treaties address cybersecurity. Then in 2015, the United States passed the Space Act to address the commercial exploration and exploitation of extraterrestrial resources with several other countries following suit: Luxembourg, Japan, China, India, and Russia.[37]

But none of these laws address cybersecurity on a worldwide or outer space scope. Therefore, not surprisingly, the United Nations adopted Resolution 74/247 creating an ad hoc committee charged with drafting a "Cybercrime Treaty" in May 2021.[38] The Cybercrime Ad Hoc Committee is an "intergovernmental committee of experts, representatives of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes."[39] This ad hoc committee is tasked with "taking into full consideration existing international instruments and efforts at the national, regional and international levels on

combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime."[40] It is unclear at this time whether the ad hoc committee will include outer space in the regulations of the Cybercrime Treaty.

One would hope that national and international laws are changed and updated to include cybersecurity of cyberspace and outer space critical infrastructure. Since the dawn of time when man first experienced conflict with neighbors, conflicts have been fought over land, sea, and then air. In modern times, conflict is being fought over cyberspace as cybercriminals and aggressor nations infiltrate private and public computer and network systems. Conflict between nations is also involving critical infrastructure in outer space.

Attorneys are advocates for their clients. But there is a reason why William Shakespeare so famously wrote, "The first thing we do, let's kill all the lawyers" in *Henry VI,* Part 2, Act 4, Scene 2. This often-quoted line is used as a joke regarding lawyers, or worse, misinterpreted. We may never truly know what Shakespeare meant, but it is clear that lawyers in his time had an impact, whether for better or worse.[41] R2-D2 and Captain Kirk are protagonists of their fictional worlds and yet used cyberspace infiltration for good. But in the hands of a cybercriminal, cyberattacks can lead to nothing short of a Death Star attack. It is incumbent upon our profession to be aware and advise our clients and the public of the importance of cybersecurity as our eyes turn to outer space and interactions in cyberspace. **TBJ**

NOTES

1. *Star Wars,* Encyclopedia Britannica (May 25, 2022), https://www.britannica.com/topic/Star-Wars-film-series.
2. *Gene Roddenberry,* Encyclopedia Britannica (Oct. 20, 2021), https://www.britannica.com/biography/Gene-Roddenberry.
3. Michael Aaron Dennis and Robert Khan. *Internet,* Encyclopedia Britannica (April 7, 2022), https://www.britannica.com/technology/Internet.
4. Michael A. Froomkin, *Government Data Breaches,* Berkeley Technology Law Journal, Vol. 24, No. 3 (2009), pp. 1019, 1022, JSTOR, https://www.jstor.org/stable/24118272?read-now=1&seq=1.
5. *Id* at 1019-1059.
6. David Bisson, *The OPM Breach: Timeline of a Hack, The State of Security* (June 29, 2015), http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/.
7. Jedidiah Bracy, *21.5 Million Breached In Second OPM Hack; Director Resigns*, Privacy Tech (July 10, 2015), https://iapp.org/news/a/21-5-million-breached-in-second-opm-hack/.
8. Nate Lord, *Top 10 Biggest Government Data Breaches of All Time in the U.S.*, Digital Guardian (October 6, 2020), https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time.
9. *Cost of Data Breach Report 2020*, pp. 8, 12, Ponemon Institute, IBM Security, https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.
10. Michael A. Froomkin, *Government Data Breaches,* Berkeley Technology Law Journal, Vol. 24, No. 3 (2009), pp. 1019, 1022, JSTOR, https://www.jstor.org/stable/24118272?read-now=1&seq=1.
11. Jenni Bergal, *Florida Hack Exposes Danger to Water Systems.* The Pew (2021, March 10), Retrieved April 13, 2022, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems.
12. Zoe Strozewski, *U.S. Airport Hit With Cyberattack Over Ukraine: 'No One is Afraid of You,'* Newsweek (March 29, 2022), https://www.newsweek.com/us-airport-hit-cyberattack-over-ukraine-no-one-afraid-you-1692903.
13. *Cost of Data Breach Report 2020*, pp. 8, 12, Ponemon Institute, IBM Security, https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.
14. Paul Lipman, *4 Critical Challenges to State and Local Government Cybersecurity Efforts (Industry Perspective),* Government Technology (July 8, 2015), https://www.govtech.com/opinion/4-critical-challenges-to-state-and-local-government-cybersecurity-efforts.html.
15. Amiah Taylor, *There's a Huge Surge in Hackers Holding Data for Ransom, and Experts Want Everyone to Take These Steps*, Fortune (February 17, 2022), https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/.
16. CISA (2021). *Stop Ransomware: Resources*, https://www.cisa.gov/stopransomware/resources.
17. Ellen Cranley, *8 cities that have been crippled by cyberattacks—and what they did to fight them*, Business Insider (January 27, 2020), https://www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1#baltimore-maryland-2.
18. TEX. H.B. 3892, 87th. LEG., R.S. (2021).
19. K. Samra, IBM survey: *Only 38% of State and Local Government Employees Trained on Ransomware Prevention.* IBM Newsroom (February 27, 2020), https://newsroom.ibm.com/2020-02-27-IBM-Survey-Only-38-of-State-and-Local-Government-Employees-Trained-on-Ransomware-Prevention.
20. Kristy Sadler, *Study: 90 Percent of New Skills are Lost After Training.* Synapse (February 22, 2016), https://getsynapse.com/blog/study-90-percent-of-new-skills-are-lost-after-training/#:~:text=Research%20conducted%20by%20Eduardo%20Salas,practical%20follow%2Dups%20or%20assessments.
21. *How Geospatial Intelligence is Providing Vital Insights into Russia's Invasion of Ukraine*, Hub (March 14, 2022), https://hub.jhu.edu/2022/03/14/michael-ard-john-oconnor-geospatial-intelligence/#:~:text=It%20has%20many%20advantages%3A%20Geospatial,to%20do%20with%20social%20media.
22. *UCS Satellite Database*, Union of Concerned Scientists (December 8, 2015), https://www.ucsusa.org/resources/satellite-database.
23. *Id.*
24. Matthew Scholl and Theresa Suloway, *Introduction to Cybersecurity for Commercial Satellite Operations*, NISTIR 8270, 2nd Draft, pp. 4 (February 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8270-draft2.pdf.
25. *Id.*
26. *Id* at p. 6.
27. Josh Lospinoso, *Space Race Needs Better Cybersecurity*, The Hill (January 13, 2022), https://thehill.com/opinion/cybersecurity/589542-space-race-needs-better-cybersecurity/.
28. *Q: What is the Mission of the U.S. Space Force?* United States Space Force, https://www.spaceforce.mil/About-Us/FAQs/Whats-the-Space-Force/
29. Josh Rogin, *A Shadow War in Space is Heating Up Fast*, The Washington Post (November 30, 2021), https://www.washingtonpost.com/opinions/2021/11/30/space-race-china-david-thompson/.
30. *Critical Infrastructure Sectors*, Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors.
31. Space Infrastructure Act of 2021, H.R. 3713, 117th Cong. (1st session 2021), https://www.congress.gov/bill/117th-congress/house-bill/3713/text?r=3&s=1.
32. *Uphold International Law*, United Nations, https://www.un.org/en/our-work/uphold-international-law.
33. *Id.*
34. *The Outer Space Treaty Has Been Remarkably Successful—But is it Fit for the Modern Age?* The Conversation (January 27, 2017), https://theconversation.com/the-outer-space-treaty-has-been-remarkably-successful-but-is-it-fit-for-the-modern-age-71381.
35. 2222 (XXI). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies,* United Nations Office for Outer Space Affairs (1967), http: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.
36. *Space Law Treaties and Principles*, United Nations Office for Outer Space Affairs, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html.
37. Jacob Brogan, *Why are India, Luxembourg, and Other Countries Getting into the Space Race?* Slate (March 1, 2017), https://slate.com/technology/2017/03/why-are-india-luxembourg-and-other-countries-getting-into-space-exploration.html.
38. *Resolution Adopted by the General Assembly on 27 December 2019*, United Nations General Assembly, Seventy-Fourth Session (Jan. 20, 2020), http: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf ?OpenElement.
39. *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.
40. *Id.*
41. Saul Boyarsky, *'Let's Kill All the Lawyers': What Did Shakespeare Mean?* The Journal of Legal Medicine (Chicago. 1979), Vol. 12, No. 4, Taylor & Francis Group, 1991, pp. 571–74, https://doi.org/10.1080/01947649109510870.

GUILLERMO "WILL" S. TREVINO
is a member of the State Bar of Texas Computer and Technology Section and serves as a member of its council. He is a graduate of Texas A&M University (B.S. 2004), Texas Southern University Thurgood Marshall School of Law (J.D. 2007), Western New England School of Law (LL.M. 2011), and Baylor University (MBA 2021) and is enrolled in Baylor University's doctoral program in Learning and Organizational Change. Trevino is a deputy city attorney for the city of Brownsville.