Seattle Journal of Technology, Environmental & Innovation Law

Volume 12
Issue 1 *Issue 12 (2022)*

Article 4

1-19-2022

On the Horizon: Nanosatellite Constellations Will Revolutionize the Internet of Things (IoT)

Diane Janosek

On the Horizon: Nanosatellite Constellations Will Revolutionize the Internet of Things (IoT)

Cover Page Footnote

The author serves as the National Security Agency's Training Director and Commandant of the National Cryptologic School. The opinions expressed herein are those of the author alone and do not represent the opinions of the Department of Defense. She thanks her mentor, Dr. Ian McAndrew, Dean of Doctoral Programs, Capitol Technology University.

On the Horizon: Nanosatellite Constellations Will Revolutionize the Internet of Things (IoT)

Diane M. Janosek, Esq.[*]

The Internet of Things (IoT) has experienced exponential growth and use across the globe with 25.1 billion devices currently in use.[1] Until recently, the functionality of the IoT was dependent on secure data flow between internet terrestrial stations and the IoT devices. Now, a new alternative path of data flow is on the horizon. IoT device manufacturers are now looking to outer space nanosatellite constellations to connect to a different type of internet. This new type of internet is no longer terrestrial with fiber cables six feet underground. It is now looking up, literally, 200 to 300 miles above the earth, to communicate, connect, and transmit data. Remarkably innovative, nanosatellites are the opposite of typical or historically sizable satellites. Nanosatellites are quite small, sometimes just the size of a shoebox. These extremely small satellites are rugged enough to remain in orbit for two to five years, all while communicating ubiquitously back to earth. These low-cost solutions to space technologies are now seen as a viable alternative to traditional terrestrial-based internet for IoT's device needs.

These low-cost satellites have significant benefits. For one, they have lowered the barrier to entry. Also, due to their design for purpose, functionality of nanosatellites can be tailored to purchasers' needs as part of the design process, from more sophisticated kitchen appliances to tracking safari animals. Tailoring generally results in a higher-than-average return on investment, thus making tailored satellites more attractive to both investors and industry alike.

---

[*] The author serves as the National Security Agency's Training Director and Commandant of the National Cryptologic School. The opinions expressed herein are those of the author alone and do not represent the opinions of the Department of Defense. She thanks her mentor, Dr. Ian McAndrew, Dean of Doctoral Programs, Capitol Technology University.

[1] Matt Fleischer-Black, *How to Address Intensifying Enterprise IoT Security Risks*, CYBERSECURITY LAW JOURNAL (Oct. 7, 2020), www.cslawreport.com

Many companies across multiple countries recognize the value of nanosatellites. France and Spain are ahead of the curve for space based IoT device connectivity. With this new technology, the investment in the field of nanosatellites has exploded. The current U.S. commercial and defense investment in space, in all orbits, is $350 billion annually, and it is expected to grow to $1 trillion or more by 2040.[2] This article will reveal that innovation in space technology has accelerated investments in space by multiple countries, investors, and industry. Likewise, there is a growth of IoT devices in the United States with more devices being purchased, more functionality per device, and better transmission. These approaches seek to satisfy the exponential demand for data, secure transmission, and global internet access, and this article will address why there is an increasing demand.

Indeed, a new era of data flow to and from "things" may quite well result in a "satellite network of things" in place of an IoT in the near future. Countries are realizing data transmission may best be from space, or at least optimized when combined with terrestrial internet communications. Using nanosatellite constellations to satisfy this demand is transformational. Nations are all reaching this same conclusion and reckoning that space is truly the next frontier that can change one's trajectory to world domination in space and economic prosperity. Both France and Spain have invested in this new arena with the use of nanosatellite constellations imminent for IoT devices, while the United States is poised to learn from their experience approach. Without a doubt, the U.S. world leadership position will be further solidified if it supports and promotes, as part of its research and development, its nanosatellites.

Nanosatellite constellations are the future of IoT as early concepts are now in research, development, and now production. This is the space, literally outer space, to watch.

I. INTRODUCTION

The IoT industry is booming with 25.1 billion internet connected devices in the world, and this number does not include mobile telephones.[3] According to Gartner's research, the volume of IoT devices in global use is expected to grow by 17% to 31% annually for the next ten years.[4]

At the same time, the growth of IoT has driven the increased utilization of space assets to control and monitor IoT devices. The emergence of ubiquity, having satellites in orbit and being "everywhere," has accompanied this dramatic investment in the commercialization of

---

[2] *Investing in Space Exploration*, MORGAN STANLEY (July 24, 2020), https://www.morganstanley.com/ideas/investing-in-space [https://perma.cc/8G3B-KC67].

[3] IoT devices are estimated to account for 30 percent of networked-connected endpoints, not including mobile phones. Fleischer-Black, *supra* note 1.

[4] Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020, GARTNER, INC. (August 29, 2019), https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io [https://perma.cc/7D6M-XH3L]. Specific estimates in the 2019 report are: "Utilities will be the highest user of IoT endpoints, totaling 1.17 billion endpoints in 2019, and increasing 17% in 2020 to reach 1.37 billion endpoints. 'Electricity smart metering, both residential and commercial will boost the adoption of IoT among utilities [....]'" *Id.* The report also notes that building automation will have the largest growth rate in 2020 by 42%. *Id.*

space.[5] This expansion and innovation in commercial space has opened the door for IoT to increase their footprint where terrestrial internet does not exist. With affordable and accessible launch vehicles for smaller satellites, IoT can truly explore previously closed doors. The technological innovation of smaller satellites, launch access, and tailored functionality, offer much promise in the new world of the IoT.

There are now options for IoT devices to connect to the internet, a company's intranet, cloud services providers, and/or dedicated networks derived from dedicated satellites. Because of the relative affordability of having a dedicated network from dedicated satellites, the production and sales of nanosatellites to global customers, including IoT manufacturers, has grown exponentially.[6] Like IoT devices, nanosatellites have unparalleled functionality and can be tailored from the ground for a very narrow purpose. So yes, these devices are in high demand, and are taking on many of the functions heretofore performed solely by the internet, which begs two questions: whether IoT regulation requiring cybersecurity protocols should be expanded to nanosatellite IoT use, and whether IoT devices residing on satellite communications will make data transmission more secure. As there is no current consensus, the world is watching, especially industry, how this evolves. Each country may approach it differently in terms of regulation. So, watch this space!

Significant benefits arise from the low cost of nanosatellites, beginning with a lower barrier to entry into the IoT device marketplace and the potential profit with expanded sale of IoT devices in rural areas where there is no terrestrial internet. With functionality tailored to the IoT manufacturers' needs, the return on the investment is higher, and many companies across multiple countries are recognizing the value of nanosatellites. The field is now exploding.[7]

By avoiding terrestrial connections, subject to known cyber vulnerabilities and hacking exploitations, will smaller satellites, which avoid the initial terrestrial internet make data traffic more secure?[8] If so, will the "Internet of Things" become known as the "Satellite Array of Things" and be preferred by manufacturers and consumers alike? How powerful could this new paradigm be if cybersecurity is sustained or increased, especially if the United States seizes the temporal opportunity to take the global lead?

II. BACKGROUND

[5] *See id.*
[6] *Id.*
[7] Christopher Mims, *The Tiny Satellites That Will Connect Cows, Cars and Shipping Containers to the Internet*, WALL STREET JOURNAL (Jan. 9, 2021), https://www.wsj.com/articles/the-tiny-satellites-that will-connect-cows-cars-and-shipping-containers-to-the-internet-11610168400 [https://perma.cc/BY8D-G6UF].
[8] Adam Lowenstein, *Apps for popular smart home devices contain security flaws*, TECH XPLORE (Sept. 24, 2021), https://techxplore.com/news/2021-09-apps-popular-smart-home-devices.html [https://perma.cc/H8XR-53R3].

A. What Is IoT And What Is the New Law on IoT?

"The IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or external environment."[9] There are thousands of types of IoT devices; a Palo Alto Network report identified 8,355 different "device types."[10] Examples include:

- Security cameras;
- Printers;
- Conference room tablets;
- Remote property sensors;
- Coffee makers;
- Door bells; and
- Door openers.

While IoT devices have a wide range of potential applications, IoT devices generally do not have a robust capability to protect the data and information being transmitted by the device.[11]

In late 2020, the United States passed its first Internet of Things act entitled "IoT Cybersecurity Improvement Act."[12] The goal of the inaugural federal act in this space is to achieve a more secure U.S. supply chain and manufacturing resiliency, which rests on operational visibility, cyber awareness, and best practices in the areas of safety, auditability, and compliance.[13] This "IoT Cybersecurity Improvement Act" aimed to address the protection shortfalls in these devices. Before that could happen, however, the legislators, with industry input, had to distill the existing complex field of IoT into a common description and definition. Merely coming to consensus on one definition was an accomplishment.

> The "IoT Cybersecurity Improvement Act" defines IoT as:
> devices that-
>
> (A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which identification and implementation of cybersecurity features is already well understood; and

---

[9] *Gartner Glossary*, GARTNER, INC., https://www.gartner.com/en/information-technology/glossary/internet-of-things (last visited Oct. 19, 2021, 2:52 pm) [https://perma.cc/CR5Q-5R2K].
[10] Fleischer-Black, *supra* note 1.
[11] *Id*.
[12] Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, 15 USC 278g-3a [hereinafter IoT Improvement Act].
[13] *See* Jeremy Kirk, *First Federal IoT Security Legislation Becomes Law*, BANK INFO SECURITY, (Dec. 8, 2020, https://www.bankinfosecurity.com/first-federal-iot-security-legislation-becomes-law-a-15539 [https://perma.cc/9Y2A-ZGAP].

> (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor.[14]

With this common definition and scope, the IoT Cybersecurity Improvement Act next moved to achieve greater data protection and cybersecurity in IoT devices. Recognizing it was best to start with a lofty but achievable goal, Congress started with IoT products the U.S. government will be buying.[15] The stated goal is to establish minimum security standards for IoT "devices owned or controlled by the Federal Government, and for other purposes."[16] Starting with devices purchased by the federal government, Congress reasoned, would lead to a "trickle down" approach over time to the majority of, if not all, devices, as IoT devices would ultimately be in the Department of Defense supply chain or be closely associated with it and would need the required security features to operate in their interactions with the federal government.[17]

Senators unanimously supported the legislation, and Senator Mark Warner of Virginia stated: "[m]ore and more products and even household appliances today have software functionality and internet connectivity... few incorporate even basic standards and protection."[18] Now with new mandates levied on IoT manufacturers desiring to sell to the federal government, states are looking to do the same. Recently, California and Oregon enacted legislation to forbid the sale of devices that do not have "reasonable" baseline security measures.[19] In due time, as more states review the security vulnerabilities in IoT devices, they are likely to introduce legislation covering IoT devices sold locally. Potentially, in just a few years, all IoT manufacturers will have these minimum-security features designed into the end-product so that there are no restrictions on markets in which to sell. The federal IoT legislation should achieve its objective to raise the bar on IoT's enabled cybersecurity features.

Remarkably, this legislation was welcomed by all parties, legislators, consumers, and manufacturers alike. As the minimum standards were achievable, there was no appetite or desire to contest the mandate. In some

---

[14] Signed by former President Donald Trump, it is the first U.S. federal law addressing IoT security. *Id.* The signing of the Act sets into motion minimum security requirements for federal agencies addressing the risk associated with IoT devices. *Id.* The requirements focus on four areas: security development, identity management, patching, and configuration management. *Id.* IoT Improvement Act, *supra* note 12.

[15] Ray O'Farrell, Executive Vice President and Chief Technology Officer, VMware: "VMware commends the bipartisan leadership of Senator Mark Warner and Senator Cory Gardner in introducing IoT security legislation. The bill includes reasonable security recommendations for the federal government to consider when purchasing IoT-related and edge computing devices. This legislation is an important, bipartisan step forward in promoting a secure federal IoT ecosystem." Mark Warner et al., *IoT Cybersecurity Improvement Act - Fact Sheet*, SCRIBD, https://www.scribd.com/document/355273144/IoT-Cybesecurity-Improvement-Act-Fact-Sheet#from_embed [https://perma.cc/J67Y-4SEH].

[16] *Id.*

[17] *Id.* at Section 2(3) "the strength of the cybersecurity of the Federal Government and the positive benefits of digital technology transformation depend on proactively addressing cybersecurity throughout the acquisition and operation of Internet of Things devices by the Federal Government."

[18] Justin Katz, *Senate Passes IoT Cybersecurity Bill*, FEDERAL COMPUTER WEEK (Nov. 18, 2020), https://fcw.com/articles/2020/11/18/iot-cyber-bill-passes-senate.aspx [https://perma.cc/28KM-7NPT].

[19] Matt Fleischer-Black, *NIST's New IoT Standard: Boosting Security as States Launch Laws*, CYBERSECURITY LAW JOURNAL, (May 4, 2020).

cases, manufacturers will naturally exceed the minimum requirements attempting to market to the discriminating consumer seeking quality and embedded security features.

Several leaders in the field and impacted manufacturers have advocated for and endorsed the IoT legislative approach.[20] Below are highlights by leaders in the field and impacted manufacturers advocating and endorsing the IoT legislative approach: Jonathan Zittrain, Co-Founder of Harvard University's Berkman Klein Center for Internet & Society, praised the legislation and said:

> Internet-aware devices raise deep and novel security issues, with problems that could arise months or years after purchase, or spill over to people who are not the purchasers. This bill deftly uses the power of the Federal procurement market, rather than direct regulation, to encourage Internet-aware device makers to employ some basic security measures in their products[21]

Similarly, Denelle Dixon, Chief Business and Legal Officer at Mozilla, stated: "This bill makes important strides in refocusing attention on how to secure the government's systems and networks. [These] reforms help safeguard the vast amounts of personal and sensitive information that the government holds but would also help to secure the products that people use every day."[22] Another supporter of the legislation was Josh Corman, Director of Cyber Statecraft Initiative, Atlantic Council. He agreed that

> Our dependence on connected technology is growing faster than our ability to secure it … we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic, and national security. Poor cyber hygiene represents a public health issue – and even threat to human life. It is encouraging to see what the federal government can do to raise the bar (both for their use and the marketplace). We know other countries and private sector initiatives are waking up to the need [to secure technologies].".[23]

In summary, the United States supports innovation in technology, but desires that IoT devices have basic cybersecurity features. At the end of the day, Americans' data privacy and confidentiality should be assured, as they may connect to up to a dozen IoT devices daily. The IoT legislation

---

[20] *See* Mark Warner et al., *IoT Cybersecurity Improvement Act - Fact Sheet*, SCRIBD, https://www.scribd.com/document/355273144/IoT-Cybesecurity-Improvement-Act-Fact-Sheet#from_embed [https://perma.cc/J67Y-4SEH].

[21] *Id.*

[22] *Id.*

[23] Also, Michelle Richardson, Deputy Director of the Freedom, Security and Technology Project, Center for Democracy and Technology opined: "We urgently need to start securing the Internet of Things and starting with the government's own devices is an important first step. This legislation will push government devices to meet modern security standards and ensure that researchers who act in good faith can independently verify the security of those devices. We hope that Congress will consider this proposal soon and look forward to a discussion about the security of government systems, where the market for Internet of Things devices is headed, and how independent research can contribute." *Id.*

is a step in the right direction, and many agree it achieved the right balance.[24]

B. Are Cybersecurity Risks Common in IoT?

IoT devices are designed for unique purposes and applications. Generally, their capabilities are not necessarily robust enough to incorporate more sophisticated cybersecurity protocols.[25] As such, cybersecurity risks are common in IoT. The challenges and security threats that have arisen are a direct result of the ubiquitous nature and "enthusiastic" adoption of IoT across business enterprise systems.[26]

The IoT field has an element of regulatory complexity. According to Ed McNichols, of Ropes & Gray, "regulation in the U.S. is done primarily sector by sector," but IoT is different as it crosses multiple sectors.[27] Chemical, nuclear, financial, medical, and defense industries all use IoT. With IoT cutting across all of these, regulation and oversight are muddled.[28] Spanning various sectors yields fragmentation, which makes universal regulation across sectors unlikely. Notwithstanding the importance of cyber-secure IoT devices for both the economy and the consumer, there is not one approach for cybersecurity protocols for all IoT devices.[29]

Another area of a common cybersecurity risk for IoT is the lack of rigorous protocols, such as firewalls. IoT devices usually do not transmit high value data such as financial information transmitted to and from banks.[30] The lack of protocols brings along a false sense of security. For example, typically the data IoT devices transmit, while sensitive, are generally not a company's highly valued data. Thus, if the data transmission is breached, the risk will be deemed low, which is not necessarily true. The IoT devices can often provide the avenue to a company's crown jewels, which is where the danger sets in. "IoT devices are low hanging fruits for attackers to get into a company's IT infrastructure," says May Wang, a senior engineer at Palo Alto Networks.[31]

Another common cybersecurity risk is when a consumer buys a low-tech IoT device, also known as plug-and-play. Manufacturers generally "do not have many ways to communicate about a patch or a fix."[32] McNichols's concern is that IoT is not maintained in the same way as

---

[24] This measured approach has been applauded, and now there is an eye to seeing where regulation may creep as IoT device manufacturers embrace nanosatellite constellations for their operational success.
[25] Fleischer-Black, *supra* note 1
[26] *Id.*
[27] Matt Fleischer-Black, *NIST's New IoT Standard: Inspiring a Wave of New Device Security Guidance*, CYBERSECURITY LAW JOURNAL (Mar. 11, 2020), www.cslawreport.com.
[28] *Id.*
[29] *Id.*
[30] Currently, IoT for banking is limited and is primarily for single transactions. No bank would solely rely on IoT to secure their data for all their customers but would rather secure the systems themselves. *See* HOW THE FUTURE OF BANKING WILL RELY ON IOT, https://www.iotforall.com/how-future-banking-relies-on-iot, Kayla Matthews, (last visited March 14, 2019) [https://perma.cc/M7KQ-G6G6].
[31] Fleischer-Black, *supra* note 1.
[32] Fleischer-Black, *supra* note 1. Even with more expensive items, updates may be available but not initiated by the consumer due to lack of knowledge.

software is maintained, such as a software update notice in one's laptop.[33] Vulnerabilities will arise as users cannot or may not update the devices. The failure to update or patch "gives hackers a roadmap to get into the device."[34]

Finally, vulnerability researchers reported multiple, validated findings with IoT, or smart coffee machines. These coffee makers gave hackers the route to home networks, also known as a "back door," which then allowed access to other devices on the home network.[35] An early discovery of the vulnerabilities of one device manufactured by Mr. Coffee was helpful for the industry as it raised concerns with basic kitchen and home appliances.[36] The attention led to follow-on work by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST).[37] Some academics even suggested it led to the initial drafting of the IoT Cybersecurity Improvement Act of 2020.[38]

C. What Are the Top Attacks to IoT?

As mentioned above, IoT devices are not necessarily robust enough to incorporate cybersecurity features and later software updates. As one would expect, concurrent with rapidly expanding sales and usage of IoT devices with cybersecurity weaknesses, there has been a marked increase in cybersecurity hacking incidents. After a consumer purchases a product and plugs it in at home, the IoT device may collect, contain, or transmit data. This data would be appropriate to the nature of the device, such as health and fitness monitoring, and pulse monitoring.[39]

The findings of the Palo Alto Networks' "2020 Unit 42 IoT Threat Report," were alarming, but not unexpected.[40] Their findings reveal that IoT attacks result from:

- 41% exploiting device vulnerabilities, which included injection and overflow attacks;
- 33% attacking via malware, botnets and ransomware;
- 13% attacking compromised passwords, mostly due to exploits of one's failure to change default passwords; and
- 13% of attacks target users through phishing and similar tactics.[41]

---

[33] *Id.*
[34] *Id.*
[35] Id.
[36] *Id.*
[37] *Id.*
[38] IoT Improvement Act, *supra* note 12.
[39] Weber, Betsy, *Fitbit, Social Media and the Internet of Things*," Just Practicing Blog (Mar. 29, 2015), https://www.justpractising.com/the-future/fitbit-social-media-and-the-internet-of-things/ The author described her FitBit as an IoT device even though "most people who use it don't know." She states, "In basic terms, the FitBit tracks my movements and shares this with a special App I have on my iPhone. It compares the movement data with data about my height, weight, stride length and communicates this information to me primarily in the measurements of daily steps walked against a target I set." [https://perma.cc/T3CL-8C5P].
[40] Fleischer-Black, *supra* note 1.
[41] Anand Oswal, *Announcing IoT Security: No Organization is Protected Without It*, https://www.paloaltonetworks.com/blog/2020/06/network-iot-security/ Embedded Link to 2020 Unit IoT Threat Report: https://unit42.paloaltonetworks.com/iot-threat-report-2020/ fig. 2 (2020). [https://perma.cc/STS2-BD8Z]; [https://perma.cc/47L5-GJKQ]

The common issue rests on a common practice: 98% of IoT device traffic on enterprise customer networks "remain unencrypted."[42] For example, cameras capture photography and videos. These cameras are connected to an unencrypted network to transmit digital data which raises hacking risks.[43] Therefore, cybercriminals use these low-tech, low-threat IoT devices as the means to a company's network, where the more valuable or lucrative data is accessible. Low-tech is no longer low risk, as one hack of an IoT device can compromise a business's most sensitive data or intellectual property.

A notable IoT breach occurred in 2017 at an unnamed casino in Las Vegas, where a connected thermometer in one of the aquariums became unsecured.[44] While this was a wake-up call to some, one can imagine that not all thermometer consumers were made aware of the product's vulnerability so as to make course corrections and secure such "stepping stones," to decrease the risk of cyber-attacks.[45] The "2019 Cybersecurity Readiness Review" reported that adversaries stole up to $6 billion in intellectual capital from the industry that supports the United States Department of Defense.[46] While the $6 billion was not all from IoT cyber-attacks, IoT devices can be the "weakest link." As such, it is no surprise that manufacturing and telecommunications industries and Congress all overwhelmingly supported the IoT Cybersecurity Improvement Act of 2020."[47]

Researchers recognize that IoT and device vulnerability concerns are rising and are now exploring if space-based internet can increase security. With decreased terrestrial connections, there should be reduced hacking into home networks where IoT devices currently connect.

III. COMMERCIALIZATION OF SPACE WITH NANOSATELLITES

A. What Are Nanosatellites?

Satellites are not new, but nanosatellites are. According to NASA, smallSats, CubeSats, and nanosatellites "vary depending on the application; some you can hold in your hand while others, like Hubble, are as big as a school bus." [48]NASA said they can have a mass less than 180 kilograms, which it compared to a kitchen refrigerator. So, there is much variety.[49]

---

[42] Fleischer-Black, *supra* note 1; *See also* original report accessible at: IoT Security: No Organization Is Protected Without It (paloaltonetworks.com).

[43] Another example is "the TV in the CEO's office" and whether connected to the internet on the "same network as financial systems. *Id.*

[44] Fleischer-Black, *supra* note 1.

[45] Palo Alto senior distinguished engineer May Wang first used the term steppingstones and was quoted in Fleischer-Black, *supra* note 1.

[46] *See* GLOBAL SECURITY, Richard V. Spencer, *Secretary of the Navy Releases Cybersecurity Readiness Review,* https://www.globalsecurity.org/security/library/news/2019/03/sec-190312-nns01.htm (March 12, 2019) [https://perma.cc/F67A-DL3C].

[47] IoT Improvement Act, *supra* note 12.

[48] *See* Elizabeth Mabrouk *What are SmallSats and CubeSats*, NASA, (2015), https://www.nasa.gov/content/what-are smallsats-and-cubesats [https://perma.cc/VE3Q-4AF7].

[49] *Id*

According to the Union of Concerned Scientists, the total number of satellites in operation today is 2,787.[50] Of this number, the United States operates 1,425, but this number changes monthly.[51] The number is rising exponentially with nanosatellites being launched monthly into Low Earth Orbit (LEO), resulting in greater ease and lower cost. Back in 2017, the largest challenge recognized by researchers to full adoption was the unavailability of launch vehicles.[52] In 2021, commercial launch vendors such as SpaceX have overcome that challenge .[53] The new generation of nanosatellites launched by SpaceX is located in LEO, between 200 and 400 miles from the Earth. Later launches may be deployed at 710 miles, but that is still considerably closer to Earth than those launched in geostationary orbit (GSO) at 22,000 miles.[54]

The difference in distance helps dramatically with latency, as the shorter distance makes satellite internet more feasible. According to Elon Musk, SpaceX's Starlink has "existing connections" which lag hundreds of milliseconds, but with "latency below 20 milliseconds…somebody could play a fast-response video game at a competitive level."[55] With the dramatic improvement in time, options abound for satellite-based IoT devices.

Nanosatellite constellations are the future of IoT as early concepts are now in research, development, and production stages.[56] Designs of a "nanosatellite constellation" have come a long way since 2017, when the "conceptual design" for use "as an IoT communications platform" was

---

[50] *UCS Satellite Database*, Union of Concerned Scientists, (Dec 8, 2005), https://www.ucsusa.org/resources/satellite-database [https://perma.cc/EBR8-T25Y]. Total number of operating satellites is 2,787, and here is breakdown by country: United States 1,425; Russia 172; China 382, and all others at 808. These 2,787 satellites are flying in the following orbit:

- LEO/Low Earth Orbit: 2,032 (200 to 400 miles in altitude)
- MEO: 137
- Elliptical: 58
- GEO/Geostationary: 560 (22,500 miles in altitude)

[51] The breakdown by type of the total 1,425 US satellites is Civil 33; Commercial 1,011, Government 173, and Military 208. *Id.* Jon Kelvey, *SpaceX Wants to Conquer the Internet*, AIR & SPACE MAG. (Oct. 2020), https://www.airspacemag.com/space/spacex-wants-wire-world-180975837/ [https://perma.cc/5QG9-MEQ2] (opining the limitations of LEO is that each LEO satellite can only see 2% of the world).

[52] A. Narayanasamy, Y. A. Ahmad, & M. Othman, *Nanosatellites constellation as an IoT communication platform for near equatorial countries*, IOP CONF. SERIES: MATERIALS SCI. & ENG'G (2017), https://iopscience.iop.org/article/10.1088/1757-899X/260/1/012028 [https://perma.cc/TK2Z-HAQG] (which read, "The absence of sufficiently small or inexpensive launch vehicles for the delivery of nanosatellites to orbit.").

[53] Patrick Nelson, *Satellite-based internet possible by year-end, says SpaceX*, NETWORK WORLD, https://www.networkworld.com/article/3398940/space-internet-maybe-end-of-year-says-spacex.html [https://perma.cc/9G9A-86N8].

[54] *Id.*

[55] *Id.*

[56] "In recent years, the space industry has seen significant growth in numbers of sub 10kg satellite platforms now known more broadly in the industry as nanosatellites. Nanosatellites potential applicability is driven by flourishing technologies miniaturization in the consumer electronics market and commercialization of space. Currently nanosatellite mission operations are limited in both lifetime and maneuverability due to limitations in on board propulsion technologies. Further enhancement of mission operations relies on more effective integration of current reaction-mass-based propulsion technologies and further development of miniaturized propulsion systems." Macario Rojas, *Design Considerations for LEO Nanosatellite Propulsion Technologies*, University of Manchester (2017).

first reported. [57] The dramatic development of space asset manufacturing is a testament to the confidence level of the return on the investment.

Today, space asset investment is booming. The Grand View Research Market, a research firm, predicts that the global market will grow to more than $645 billion by 2027.[58] There is both optimism and confidence. For example, in 2021, a small U.K.-based startup called Lacuna Space placed three communications satellites in orbit and two more on the way–with two being the size of a briefcase and the third as big as a shoebox.[59] Like nearly all nanosatellite constellation startups, Lacuna Space needs to deploy dozens more satellites to cover *the entire Earth at all times*.[60] Presently, many customers testing the company's technology can only connect to the satellite two to four times a day. Customers accept this timing limitation. "For applications like monitoring remote infrastructure, such as the penguin cameras, that's often enough," according to Rob Spurrett, Lacuna Space's chief executive and founder.[61]

Both manufacturers and researchers across the globe are exploring the use of nanosatellites for IoT.

With reduced latency time to milliseconds and lower costs for satellite internet, many innovative and creative approaches use cases are being researched. While the field is still in its infancy, early indicators suggest much promise. As the saying goes, "the sky is the limit." In this case, rather "deep space" is the limit.[62]

B. Uses of Nanosatellites

Nanosatellite constellations are changing earthly endeavors, and thus, the future. The exemplar below provides a creative use of a nanosatellite. What a nanosatellite may not have in terms of 24/7 coverage, it compensates for with lower-cost and "just what is needed"' functionality. Nanosatellites and IoT devices are being used in Antarctica for penguin tracking; where humans rarely go, but where status updates are routinely needed.

In the shadow of giants like SpaceX, more than a dozen startups are building their own globe-spanning networks of nanosatellites, enabling a new kind of everywhere, all-the-time connectivity for people, animals and assets on Earth. Scientists who track the health of Adélie penguins on the ice-covered wastes of Antarctica are managing their cameras from thousands of miles away—via tiny satellites orbiting above our heads… this evolving

---

[57] A. Narayanasamy, *supra* note 52.

[58] Jon Kelvey, *SpaceX Wants to Conquer the Internet*, AIR & SPACE MAG. (Oct. 2020), https://www.airspacemag.com/space/spacex-wants-wire-world-180975837/ [https://perma.cc/5QG9-MEQ2]. (opining the limitations of LEO is that each LEO satellite can only see 2% of the world).

[59] Mims, *supra* note 7.

[60] *Id*. (Emphasis added).

[61] According to Lacuna Space, its satellites connect to things on the ground using LoRaWAN networks which are already widely used for earthbound devices sold by Amazon and others. *Id*.

[62] Pushing all boundaries, there is even ongoing research exploring if nanosatellites can be ruggedized and used for deep space. Nacer Chahat et al., *Advanced CubeSat Antennas for Deep Space and Earth Science Missions: A Review*, IEEE ANTENNAS AND PROPAGATION MAG. (Oct. 2019), https://ieeexplore.ieee.org/document/8827280 [https://perma.cc/BTD5-B8V2]; Advanced CubeSat antennas for deep space and earth science missions: A review. *IEEE Antennas & Propagation Magazine, 61*(5), 37-46. doi: http://franklin.captechu.edu:2123/10.1109/MAP.2019.2932608 See also https://pureadmin.qub.ac.uk/ws/portalfiles/portal/174234474/IEEE_Magazine.pdf.

satellite technology… [are the] novel networks of nanosats—aka cubesats.[63]

The director of the Adélie penguin project, the Arriba Initiative, built ruggedized "low-cost cameras to withstand harsh Antarctica conditions" and to store images on SD cards that are collected once a year.[64] The cameras rely on satellite internet data transmission, and not terrestrial internet, to frequently report the camera's status, such as "low battery, covered in ice, tipped over, etc. to their keepers in London via tiny satellites."[65]

Similar to tracking penguins in Antarctica, nanosatellites are being explored for the tracking of animals in Africa as part of the Smart Parks project. Currently, an elephant collar is being tested that can track animals into "deserts, forests, and transborder parks between counties in Southern Africa" where "no other wireless" is available.[66] The elephant collar being tested in Malawi has a single battery that is expected to last ten years due to relatively low power needs, combined with the satellite connection.[67] This advancement in IoT is remarkable and reflects why "16 companies are now investing in similar types of satellites networks."[68]

The global innovation and technological advancement and sophistication are astonishing in that nanosatellites are being explored and are universally enjoying successes. On the cusp of this change is Sky and Space Global. Mr. Meir Moalem of Sky and Space Global is not shy in his quest to "bring affordable mobile services to the world." His fleet is set to be operational by 2020-2021 and will provide text, voice, and data transfer services to the Earth's equatorial regions–including much of Latin America and Africa. If successful in achieving his vision, he will have a market of up to three billion people. It is this follow-on market-share that is driving investment today.[69]

Space asset manufacturers and investors recognize the impact. "Affordable mobile services are critical for the economic and social development of many developing countries," says Mr. Moalem, who believes his nanosatellites will shake up the space-based communications market.[70] "Our total constellation costs just $150m (£108m). That is less than the cost of a single standard communications satellite. This is what we mean when we talk of a disruptive technology."[71]

Sky and Space Global is just one of several companies with big plans for space right now. "Perhaps the most ambitious is Elon Musk's SpaceX, which is aiming to build a huge 4,400-satellite constellation offering global internet coverage. It will be using its own Falcon-9 rockets to launch its fleet and plans to have the network operating by 2024."[72]

---

[63] Mims, *supra* note 7.
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Tim Bowler, *The Low-Cost Mini Satellites Bringing Mobile to the World*, BBC NEWS (Feb. 23, 2018), https://www.bbc.com/news/business-43090226, [https://perma.cc/YDA7-WMEW].
[70] *Id.*
[71] *Id.*
[72] *Id.*

Like other potentially lucrative fields, there is competition. The vision of Remco Timmermans, of Open Cosmos Head of Communications, is to "make space accessible by making space missions simple."[73] Others have this same ambition. The current U.S. investment in space is $350 billion annually and "is expected to increase to more than $1 trillion by 2040."[74] To be expected, with all these satellites, it is becoming an increasingly crowded space.[75]

Not only is space getting congested, but there is also a growing list of satellite manufacturers and investors now interested in getting in at ground zero. LEO satellites, which have an altitude of 2,000km (1,200 miles) or less above the planet, are less expensive to launch. , For example, Sara Spangelo, the CEO and co-founder of Swarm Technologies, the Mountain View, California based LEO manufacturer, stated it could soon complete the first commercially available nanosatellite constellation. [76] This constellation would enable customers to reach a satellite whenever they choose. Remarkably, Swarm has already launched forty-five satellites, thirty-six for commercial customers and the remainder experimental. The company "expects to launch [thirty-six] more from Florida on a SpaceX Falcon 9 rocket on Jan. 14, with a total of 164 aloft" by the end of 2021, and 150 of them active.[77] Swarm is keeping costs low by producing satellites that are extra small. Each one is about the size of a "grilled cheese sandwich." Swarm's satellites communicate in the VHF spectrum—adjacent to but not overlapping the spectrum used by shipboard radio systems—which allows for good signal penetration, even in cities and indoors.[78]

C. When Were Nanosatellites First Considered for IoT?

Throughout 2017 to 2019, confidence that nanosatellites could be used for IoT continued to increase. Confidence levels rose each year, as researchers continually validated predictions.

At the 6th International Conference on Mechatronics in 2017, three researchers presented their research focused on leveraging IoT for control

---

[73] Writers, S., "Interactive space simulation for nanosatellites," Feb 22, 2019, *UPI Space Daily* stating that in Paris, "Pioneer partner Open Cosmos are taking mission development to a new dimension, using a virtual reality-like simulation that replicates life in orbit for space technologies. Through an innovative combination of a plug-and-play test platform and software, the UK Harwell-based SME is slashing the time it takes for space missions to be designed and qualified for launch.") *Interactive Space Simulation for Nanosatellites*, UNITED PRESS INT'L SPACE DAILY (Feb. 22, 2019), https://www.proquest.com/wire-feeds/interactive-space-simulation-nanosatellites/docview/2184361136/se-2?accountid=28598 [https://perma.cc/V2HV-XAMC]; *Interactive Space Simulation for Nanosatellites*, THE EUROPEAN SPACE AGENCY (Feb. 19, 2019), https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Interactive_space_simulation_for_nanosatellites [https://perma.cc/C8LV-Z2NP].

[74] Stanley, *supra* note 1.

[75] The proliferation of these nanosat companies is ongoing. Aravind Ravichandran, an independent consultant in the space industry, says "At this point there's basically one IoT-from-space company per country. It's just crazy, and I don't know if you have that much demand." *See* Mims, *supra* note 7.

[76] Dr. Spangelo is a former NASA Jet Propulsion Laboratory engineer and as she says, a "failed Canadian astronaut"—she made it to her cohort's final thirty-two before being cut. *Id.*

[77] *Id.*

[78] Two years ago, Ford Motor Co. announced a partnership with Swarm. "Whatever they're working on is still under wraps." *Id.*

and communication of data from space. The researchers concluded an orbit closest to the Earth would be optimal and recommended the LEO.[79]

Affordability of space assets may seem like a paradox due to the inherent exorbitant costs to design, build, launch and maintain a satellite. Nanosatellites, however, can be less costly than terrestrial-based fiber optic cables built for traditional internet. Experts acknowledge that the internet is "expensive" to expand across the globe, especially to less-populated areas, as it involves "lay[ing] fiber optic cables and build[ing] cell towers in remote areas."[80] So widely available satellite-based internet, once envisioned in the 1990s, may no longer be a fantasy in 2021 and beyond, and less risky for investors.[81]

In 2018, Report buyer, a leading industry intelligence solution that provides all market research reports from top publishers, issued a report highlighting the versatility of the emerging nanosatellites' capabilities and relatively low costs. The report acknowledged "a new niche market dedicated to small satellites" with new players excited about the miniaturized technologies with the wide range of advanced launch technologies.[82] It reads,

> Nanosatellites and microsatellites have proven to be dynamic for embracing new developments in various sectors such as weather information and climatic research, multimedia communications, telephone and television, data distribution, transportation and logistics, navigation, safety, security, and rescue. As these satellites have paved the way for cost-effective earth observation missions along with the development of small launchers and small ground stations connected with cost-effective data distribution methods, industry participants have shifted their focus toward developing nanosatellites and microsatellites.[83]

In 2018, Sky and Space Global reported its successful "critical design review" of 200 nanosatellites called "pearls." As the world watched, Sky and Space Global then proceeded as it sought to bring internet access to underserved regions of the earth through a nanosatellite constellation .[84]

---

[79] Narayanasamy, *supra* note 52

[80] Kelvey, *supra* note 58.

[81] Investors have been wary of investing in satellite manufacturing, due to high risk of financial loss. In 2020, SpaceX Starlink's competitor, OneWeb, did declare bankruptcy. *Id.*

[82] *The Global Nanosatellites and Microsatellites Market Is Expected to Reach USD 4.97 Billion by 2025*, PR NEWSWIRE (Jan. 30, 2018), https://www.prnewswire.com/news-releases/the-global-nanosatellites-and-microsatellites-market-is-expected-to-reach-usd-497-billion-by-2025-300590128.html [https://perma.cc/A2HF-B735]. (stating that there is a widening customer base with "[i]ncreasing demand from economies such as India and Japan is contributing to the growth of the nanosatellite and microsatellite market. For instance, in the wake of miniaturization, Japan is developing strategies to tap the demand for compact satellites and aircraft.").

[83] *Id.* (stating that "[m]oreover, CubeSats, which are smaller than nanosatellites are witnessing a rise in popularity due to their shorter time to orbit and lower manufacturing costs.").

[84] According to M2 Presswire, Sky and space global started construction and integration of its network of two hundred nanosatellites to serve the world's unconnected population upon successfully completed

Then in 2019, three PhD students studying in France, the United States, and Northern Ireland collectively assessed that "[e]xtending the internet of things (IoT) networks to remote areas under extreme conditions or for serving sometimes unpredictable mobile applications has increased the need for satellite technology to provide effective connectivity."[85]

In summary, researchers now recognize that nanosatellites can, with more research and development, have a variety of functionality and application. In 2021, nanosatellites are being explored, and in some cases are even in development, across multiple industries to include:

- weather information and climatic research,
- resource management and mapping,
- multimedia communications,
- telephone and television,
- data distribution,
- transportation and logistics,
- navigation,
- safety, security, and rescue,
- agriculture,
- defense, and
- land management.

In the following sections, case studies are provided that demonstrate nanosatellite application to agriculture and land management, involving associated IoT devices for connectivity and data transmission.

Wider adoption of nanosatellite technology is coming to the United States.[86] Next is the discussion on developments in France and Spain.

IV. CASE STUDIES: FRANCE AND SPAIN NANOSATELLITES

Lessons can be learned by leading companies in two other countries: both France and Spain have supported the expanded use and exploration of nanosatellites.

A. FRANCE: ANGELS Program

In Toulouse, France, in May 2017, the French government space agency, the National Centre for Space Studies (CNES), announced a new space joint venture with "Thales Alenia Space."[87] It was a significant announcement for France, as well as the industrial partners. Thales Alenia Space was to be the supplier of the Argos Neo instrument, which would

---

the critical design review of its "pearls" nanosatellites in 2018. Jennifer Read, *Sky and Space Global Starts Construction and Integration of Its Network of 200 Nano-Satellites to Serve the World's Unconnected Population*, EMSNOW (Oct. 26, 2018), https://emsnow.com/sky-and-space-global-starts-construction-and-integration-of-its-network-of-200-nano-satellites-to-serve-the-worlds-unconnected-population/ [https://perma.cc/G2GE-2BKV].

[85] Chahat, *supra* note 62.

[86] *See* Kelvey, *supra* note 58.

[87] This joint venture was established at 67% Thales and 33% Leonardo. *Thales Alenia Space to Provide Argos Neo Instrument for French Space Agency Nano-Satellite Demonstrator, Angels*, THALES (May 18, 2017), https://www.thalesgroup.com/en/worldwide/space/press-release/thales-alenia-space-provide-argos-neo-instrument-french-space-agency [https://perma.cc/43ZT-378H].

be part of the nanosatellite demonstrator Argos Neo on a Generic Economical and Light Satellite (ANGELS) program.[88] Thales Alenia Space had an additional development partner for Argos Neo, Syrlinks, a well-respected manufacturer of radio-communications and geo-location equipment.[89] This team of talented mission partners was rounded out with the addition of the satellite manufacturer Nexeya, based in Toulouse, France.[90] The support is a clear signal that France will invest in French space companies, which will drive down risk.[91]

There was much excitement in 2017 as many saw ANGELS as the dawn of a new era, ANGELS was literally launched just three years after its press conference.[92] Overall, ANGELS was swiftly designed, developed, and manufactured, and weighed less than 50 kg.[93] 2020 was a notable year with the newest innovation of space-borne IoT.[94] Ten times smaller than its predecessors, ANGELS was designed for low cost. [95] ANGELS overcame challenges and achieved miniaturization with high-end performance, and now this "technological wonder" is increasing access to internet connectivity.[96]

The French Government had both the foresight and desire to achieve its national objectives in space through partnership. It began in

---

[88] *ANGELS (Argos Neo on a Generic Economical and Light Satellite)*, EARTH OBSERVATION PORTAL (last visited Oct 20, 2021), https://directory.eoportal.org/web/eoportal/satellite-missions/content/-/article/angels [https://perma.cc/B8JN-95YC].

[89] *Id.* (stating that "ANGELS gives a first taste of the opportunities provided by Kineis, the first constellation of European nanosatellites dedicated to IoT. Carrying a state-of-the-art ARGOS instrument, ANGELS is the operational proof of the success of the French nanosatellite sector."). Caroline Laurent, CNES's Director of Orbital Systems stated that the opening of new services and the inclusion of ANGELS in the ARGOS satellite fleet represent a new milestone in the ARGOS system success story, and that it was due to the unique partnership between CNES, Thales Alenia Space, Syrlinks and HEMERIA. *Id.*

[90] *Id; see* Thales, s*upra* note 87 (stating that "the aim of Argos Neo is to demonstrate the operational capability of a complex miniaturized instrument offering high performance on a nanosat platform.").

[91] CNES in French is "Centre national d'études spatiales." The French government space agency, CNES, manages space assets with either industrial or a commercial purpose. While its headquarters are in Paris, it operates the Toulouse Space Center and Guiani Space Center where it can service both French sand other nation's satellite launches. *See CNES – The French Space Agency*, THE MISSION FOR SCIENCE & TECHNOLOGY (last visited Oct 20, 2021), https://france-science.com/en/cnes-2/ [https://perma.cc/LD73-7NQ3].

[92] *Id.*

[93] Details were carefully considered, and Angels is carrying ARGOS Neo which was the precursor of a new generation of low-cost, highly miniaturized instruments. Earth Observatory Portal, *supra* note 88. (adding that "All the innovations developed on board of the satellite in orbit has immediate benefits for users. In practical terms, this new instrument allows the transmitters to become smaller and lighter, which opens up the range of objects inside which they can be fitted. While the ANGELS model already offers exceptional performance, the 25 similar nanosatellites of the future constellation will meet even more demanding specifications.").

[94] *See id.*

[95] *See id.* (stating that "[t]echnology offering a five-time performance increase and greater service capability ANGELS is so sensitive that transmitters on the ground can reach it with a transmission power of just 100 mW, about a fifth of the power needed by current ARGOS transmitters. It also provides access to a new frequency band, boosting the capabilities of the seven satellites in the current system. These major innovations will enable users to extend the battery life of their transmitters and reduce their size and weight. Data from the 20,000 transmitters are currently processed by the whole system, a figure that will increase to several million by 2030. For biologists, who have been using the ARGOS system with CLS for more than 40 years, this means that their studies can last longer and can include new, smaller species through suitably miniaturized transmitters.").

[96] *Id.* (stating that the addition of ANGELS to the ARGOS satellite fleet "offers new data collection capabilities. The ARGOS Neo instrument is the first of a new generation: this technological wonder has passed the challenge of miniaturization by being ten times lighter (2 kg) and three times more energy-efficient than previous generations.").

2018 when the French space agency CNES created an investment fund of "80 to 100 million euros ($95 to $119 million)."[97] The French Government's announcement is revealing: "We completely changed our approach, and we consider CNES has a very important role to play in NewSpace."[98] These efforts to achieve France's vision have placed France on the international stage as a world leader in space.

B. SPAIN: SATELIOT Partnership

"Spain has had success in nanosatellite innovation and IoT."[99] The Government of Spain wanted to be an early adopter and boost their economy, and satellite internet became a key component of the country's business economic development. The COVID-19 pandemic re-emphasized to Spain that satellite internet would and could play a major role to jump start businesses.[100] Spanish satellite manufacturer, Hispasat, and its CEO said, "any investment in the satellite industry is a contribution to growth, job creation, innovation and competition within industry."[101] Spain's mountainous landscape makes land-based internet more challenging.[102] Also, Spain is seeking to accelerate the development of 5G with a high-quality internet combining the technologies of terrestrial internet, fiber optic, and satellites. Thus, Spain made the natural choice to invest in nanosatellite innovation for IoT.

Spain's Space Agency, Instituto Nacional de Técnica Aeroespacial (INTA), is working on Sateliot, one of the country's leading satellite telecommunications operators in Spain. On December 2, 2020, the International Telecommunication Union (ITU) granted to Sateliot approval to launch a constellation of 100 nanosatellites for IoT connectivity.[103] Spain is proud that Sateliot will be the first satellite telecommunications operator to provide global and continuous connectivity to the universe of IoT under the 5G protocol. Space-based internet will soon connect to automobiles and homes.[104]

---

[97] *Id.*

[98] Henry, Caleb, *CNES Creating a Space Startup Fund*, SPACE NEWS (May. 7, 2018), https://spacenews.com/cnes-creating-a-space-startup-fund/ [https://perma.cc/ZH4S-H8U9] (stating that NewSpace is viewed as embracing innovative "firms typically running on venture capital with a mission to disrupt the space sector with new products and services.").

[99] Rachel Jewett, *Sateliot Receives ITU Approval to Launch IoT Nanosatellite Constellation*, SATELLITE TODAY, (Dec. 2, 2020), https://www.telecompaper.com/news/spains-sateliot-receives-itu-approval-for-5g-nanosatellite-launch--1364024 [https://perma.cc/7NY6-7NZ2].

[100] *Satellite Internet as a Driver of Economic Transformation in Spain*, LYNTIA.COM (2020), https://www.lyntia.com/en/news/satellite-internet-as-a-driver-of-economic-transformation-in-spain/ [https://perma.cc/3XUM-TNVT].

[101] *Id.*

[102] *Id.*

[103] Jewett, *supra* note 99.

[104] *Sateliot and Danish Gatehouse to Offer Global 5G via its LEO Nano-Satellites*, UPI SPACE DAILY, (Jul. 28, 2020), https://www.spacedaily.com/reports/Sateliot_Allies_with_Danish_Gatehouse_to_its_LEO_Nano_satellites_to_Offer_a_Global_5G_connection_999.html [https://perma.cc/7X2U-XSUB] (opining that "[t]hanks to a constellation of nanosatellites of the latest generation, located at low altitude that act as mobile towers, Sateliot is the perfect complement to the large telecommunications companies by providing them with the necessary infrastructure where terrestrial technologies do not reach.").

The combination of terrestrial-based internet and space-based internet is transformational.[105] Sateliot's nanosatellite constellation at low altitudes acts "as mobile towers in space" and increases "connectivity for the IoT beyond the limits of terrestrial infrastructure".[106]

The design, manufacturing, assembly, launching, and servicing of nanosatellite constellations takes a village. In the case of Spain, it took three countries collaborating and international approval. Sateliot is based in Barcelona, Spain, partnered with Open Cosmos, a U.K. company that operates end-to-end space missions. Open Cosmos was responsible for the design and manufacturing, Harwell Technology in the U.K. handled assembly, and Kazakhstan performed viability testing in its country's test areas.[107] Open Cosmos oversaw the launch from the Baikonur Cosmodrome in Kazakhstan by integrating Sateliot's nanosatellite into the deployer launched by the Soyuz rocket.[108] Space technology is rocket science, and Spain benefited from collaboration due to the wide-range of expertise and sub-specialties needed for success.

With Spain's interest to learn from Sateliot's early successes, it can be on the path to the world stage in space innovation.

C. Review of Case Studies

Spain and France have demonstrated the viability and the profitability of nanosatellite constellations for IoT. Additionally, both governments provided regulatory approval, which is essential in minimizing risks and increasing profitability.

These case studies demonstrate a potential for other countries to be leaders in space innovation and technology with the proper support. This course of action will make Spain a new contender in space power and non-terrestrial IoT networks.[109] The utility of non-terrestrial IoT networks knows almost no bounds.[110]

With these opportunities, Morgan Stanley estimates that satellite internet will represent 50% of the projected growth of the global space economy by 2040.[111] While satellite launchings, even nanosatellites, are

---

[105] With the ITU approval to launch, Sateliot is now permitted to coordinate the frequencies of its nanosatellite constellation with telecom operators, as well as opening talks with the space operators and public administrations to ensure frequency compatibility. Jewett, *supra* note 99.

[106] *Id. See also* Ferrer, et al. *Review and Evaluation of MAC Protocols for Satellite IoT Systems Using Nanosatellites,* SENSORS (2019), https://www.mdpi.com/1424-8220/19/8/1947 [https://perma.cc/NZZ7-826Z].

[107] *Sateliot Prepares with Open Cosmos to Launch its First Nanosatellite on 20 March,* CRABS.NAME (2021), https://crabs.name/37424364_4.html [https://perma.cc/P4BZ-MUEQ].

[108] *Id.* (stating that this nanosatellite referred to as 3B5GSAT will be "the first of three with which Sateliot will test the IoT service with 5G coverage – comprises an innovative small technology – smaller than a microwave and weighing no more than 10 kg – made up of 10x10x10 cm cubes whose standards are adapted to the function to be performed. Moreover, unlike large geostationary satellites that are almost 36,000 kilometres high, it will be in a low orbit, flying at only about 500 kilometres to ensure global IoT connectivity. It will travel at a speed of about 7 km per second, circling the Earth once every 90 minutes.").

[109] For early discussions, *see* Mark Holmes, *Clyde Space Secures New Nanosatellite Contract*, SATELLITE TODAY (2016), https://www.satellitetoday.com/innovation/2016/11/29/clyde-space-secures-new-canadian-contract/ [https://perma.cc/R4JX-45F2].

[110] *Id.* For expanded technology background, *see also* Ferrer, et al, *supra* note 106.

[111] MORGAN STANLEY.COM, *supra* note 2

expensive, offering internet service globally, especially in rural and remote locations, will help to drive down the cost due to not having to bury cables across miles.[112] These decreasing investment costs are coming at a time of tremendous appetite for the ability to transmit data globally for IoT devices.

V. THE UNITED STATES' STANDING IN ITS SPACE INVESTMENTS

The U.S. has always been a leader in space, as evidenced by having the highest number of satellites in orbit. This could change with this new international awakening to what is on the horizon. The U.S. should take deliberate steps to demonstrate support for its commercial space activities. For example, it could increase the budgets of the federal regulatory agencies to aid in swifter processing of space licenses.[113] A more welcoming approach to space will assist in sustaining and promoting economic prosperity.[114]

There is much excitement in the U.S. surrounding Elon Musk's SpaceX. However, his model will not work for smaller space technology companies without large research and development budgets. Accordingly, the U.S. Congress should look to seize the moment to take an affirmative step to zealously advocate for U.S. commercial space investments before these businesses look to other countries with less regulation. There is some positive movement as efforts are underway to relax strict licensing requirements. Specifically, these efforts aim to consolidate and streamline the regulatory framework and organizations for U.S. commercial space capabilities.[115]

While the U.S. Congress has reviewed the issue, legislation needs to be passed. On an optimistic note, legislation was previously introduced. In view of the case studies of Spain and France, there should now be momentum to pass the legislation. Specifically, in the 115th Congress, the American Space Commerce Free Enterprise Act and the Space Frontier Act included provisions to streamline the current onerous licensing process.[116] In the 116th Congress, the American Space Commerce Free

(stating that "[t]he demand for data is growing at an exponential rate, while the cost of access to space (and, by extension, data) is falling by orders of magnitude…. We believe the largest opportunity comes from providing Internet access to under- and unserved parts of the world, but there also is going to be increased demand for bandwidth from autonomous cars, the Internet of things, artificial intelligence, virtual reality, and video.").

[112] *Id.*

[113] *See* Jeff Foust, C*ommerce Department Seeks Big Funding Boost for Office of Space Commerce*, SPACE NEWS (Feb. 16, 2020), https://spacenews.com/commerce-department-seeks-big-fun [https://perma.cc/SP7Y-XF6W] (stating that the Department's desire to consolidate and hire more personnel to streamline but noting budget increase has not yet been approved.).

[114] Rachel Jewett, *SpaceX Launches Record Rideshare Mission Carrying 143 Satellites*, SATELLITE TODAY (Jan. 24, 2021), https://www.satellitetoday.com/launch/2021/01/24/spacex-launches-record-rideshare-mission-carrying-143-satellites/ [https://perma.cc/JX42-RVYA] (stating that "Spaceflight's customers included Astrocast, which will deploy a nanosatellite Internet of Things (IoT) network; a cluster of Radio Frequency (RF) mapping satellites forHawkEye 360, a Synthetic Aperture Radar (SAR) satellite for iQPS (Institute for Q-shu Pioneers of Space); and the NASA cubesat Pathfinder Technology Demonstrator-1.").

[115] Foust, *supra* note 113.

[116] *Babin Introduces American Space Commerce Free Enterprise Act*, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY (July 2, 2019), https://republicans-science.house.gov/news/press-releases/babin-introduces-american-space-commerce-free-enterprise-act [https://perma.cc/R3X6-M7GV]. *See also*

Enterprise Act of 2019 was introduced by Rep. Brian Babin, ranking member of the House Science, Space, and Technology Subcommittee on Space and Aeronautics.[117] Rep. Babin seeks to affirm American competitiveness and security and believes the U.S. could lose its "commercial space entrepreneurs, industry jobs, and innovative technology because of our slow, uncertain, and difficult regulatory process." His bill was not passed.[118]

If the U.S. Congress supports space investment through tax credits and regulatory relaxation – as France and Spain did – the U.S. will be poised to both embrace these opportunities and remain the world leader in space technology. The U.S. Congress recently rallied behind the Internet of Things Cybersecurity Improvement Act of 2020 and passed it unanimously.[119] So, there is both a precedent and optimism that there could be "Satellite IoT" legislation and a firm commitment of support.[120] The U.S. should invest in nanosatellite technology to both address the need for data transmission capacity for IoT expansion and the American industry's desire to invest in space assets.

VI. CONCLUSION: PROMOTE THE EXPANSION OF NANOSATELLITES

Innovation in space technology has accelerated investments in space by multiple countries, investors, and industries. A review of the growth of IoT devices in the U.S. reveals a voracious appetite for more devices, more functionality, and increased data transmission options. These approaches partially satisfy the exponential demand for data, secure transmission, and global internet access. France and Spain serve as examples of success.

Countries are realizing data transmission may best be from space, or at least optimized when combined with terrestrial internet communications. Using nanosatellite constellations to satisfy this demand is transformational. Nations are all reaching this same conclusion and understanding that space is truly the next frontier that can change one's trajectory to world domination and economic prosperity. Without a doubt, the U.S. world leadership position will be further solidified if, as part of its research and development, its nanosatellites also address cybersecurity and surveillance vulnerabilities.[121]

Do not wait for the horizon to get here: now is the time to prepare for the next big thing in secure digital global communications.

American Space Commerce Free Enterprise Act (H.R. 2809), 115th Cong.; S. 3277, 115th Cong. (2019). In the 115th Congress, the American Space Commerce Free Enterprise Act (H.R. 2809) and the Space Frontier Act of 2018 (S. 3277) include provisions to streamline the licensing process.

[117] *Id. See also* H.R. 3610, 116th Cong. (2019).

[118] *Id.*

[119] IoT Improvement Act, *supra* note 12(stating that it was passed Senate without amendment, and it passed the House by unanimous consent via voice vote).

[120] *Id.*

[121] Stanley, *supra* note 1.