CORPORATE ESPIONAGE BY DRONE: WHY CORPORATIONS NEED BETTER PHYSICAL AND LEGAL PROTECTIONS

E. Claire Scott[*]

[*] J.D. Candidate, 2022, University of Mississippi School of Law. The author would like to thank her friends and family for their support during the writing of this piece. She would like to dedicate this piece in memory of her great-grandmother, Annette Clemmons, who was always her biggest supporter.

INTRODUCTION

Gone are the days of traditional corporate spies, planting moles and wiretapping phones. Today, corporate espionage takes on a new form in the world of cyberspace. Due to the rise of an information-based society and cloud technology, spies are now able to gather intel without ever stepping foot into their target's office.

Corporate espionage has continually been a problem for businesses since the age of commerce began;[1] however, bad actors now have more technology available than ever to conduct espionage, physical or cyber,[2] on unsuspecting corporations. It is also more prevalent than one may think. As of 2004, "[m]ore than 50 percent of Fortune 1000 companies [admitted to having] been victims of corporate espionage," and at the time, it costed "American

[1] John A. Stone, *Seize the Day, or at Least the Trade Secrets: Protecting Trade Secrets Against Cyber Theft Using the New Jersey Trade Secret Act and the Defend Trade Secrets Act*, N.J. LAW., Dec. 2016, at 8, 8 (quoting *Famous Cases of Corporate Espionage*, BLOOMBERG (Sept. 20, 2011, 2:00 PM), https://www.bloomberg.com/news/photo-essays/2011-09-20/famous-cases-of-corporate-espionage [https://perma.cc/BA2Z-3W45]) ("For as long as there has been commerce, there has been espionage.").

[2] *See generally* Elizabeth Hanford, *The Cold War of Cyber Espionage*, 20 PUB. INT. L. REP. 22 (2014) (briefly discussing cyber espionage).

businesses approximately $200 billion annually."[3] Corporate espionage—sometimes referred to as "industrial espionage, economic espionage, and misappropriation of trade secrets"[4]—"is the practice of using [spying] techniques" for business-related gains.[5] This practice will only progressively get worse as corporate spies now have access to newer, easier-to-use, and cheaper technology—specifically, drones.

This Comment will proceed by providing a short history of corporate espionage, showing both traditional and modern espionage tactics. Though traditional spying techniques still occur, today's espionage mostly takes on a cyber form, frequently referred to as cyber espionage.[6] Hackers and other bad actors may still conduct cyber espionage, but a new threat is emerging: cyber espionage by drones. Drones allow a new medium for espionage and trade secret misappropriation as they are easily accessible, virtually undetectable, and make an already challenging situation of proving a trade secret misappropriation claim even more difficult.[7] This Comment will focus specifically on the problems and implications that arise from corporate espionage by drone. This Comment additionally provides a short synopsis of the relevant trade secret and cyber laws. Then, it will discuss the problem at hand. Drones can conduct physical attacks and cyberattacks on unsuspecting businesses,[8] and they only have reactive remedies available rather than proactive ones.[9] Drones can bypass both physical and cybersecurity measures and can easily be used to hack

---

[3] Glenna Rodgers & Scott D. Marrs, *Trade Secrets and Corporate Espionage: Protecting Your Company's Crown Jewels*, ACC DOCKET, Apr. 2004, at 60, 62. It is likely that those numbers have only risen in the past eighteen years since that statistic was analyzed.

[4] *Id.*

[5] Josh Fruhlinger, *What Is Corporate Espionage? Inside the Murky World of Private Spying*, CSO (July 2, 2018, 3:28 AM), https://www.csoonline.com/article/3285726/what-is-corporate-espionage-inside-the-murky-world-of-private-spying.html [https://perma.cc/8EW2-CBEQ].

[6] *See* discussion *infra* Section I.B.1.

[7] *See* NAT'L URB. SEC. TECH. LAB'Y, U.S. DEP'T OF HOMELAND SEC., COUNTER-UNMANNED AIRCRAFT SYSTEMS TECHNOLOGY GUIDE 6-12 (2019). This Comment will focus primarily on private action and, therefore, will not discuss any Fourth Amendment privacy claims or issues in regard to drone usage.

[8] *See id.* at 6.

[9] *See* discussion *infra* Section I.A.2.

isolated systems with remote sensing payloads.[10] Also, drones can be used for reconnaissance missions by using their camera, thermal imaging, recording, and other similar capabilities.[11] Drones are a more attractive option for bad actors as they are virtually undetectable and untraceable.[12] Even though corporations are facing this problem, there is no adequate solution available to them—legally or physically. Corporations are left defenseless against cyberattacks and espionage by drones, as the technology necessary for such security is illegal in the United States under several statutory schemes.[13]

The current legal landscape in the United States does not allow corporations to use proactive methods of protecting themselves from corporate espionage or cyber misappropriation by drones. The current system in place only allows for reactive steps, a trade secret claim,[14] which is arguably unhelpful due to the nature of the grievance—the trade secret has already been lost, likely replicated and sold, before the company discovers the intrusion. There is a better and more proactive option available for corporations, but it is illegal in the United States: counter-unmanned aircraft systems ("C-UAS").[15] Such systems allow for the detection, tracking, and sometimes, the destruction of unfriendly drones.[16] Thus, with their use, corporations could protect themselves from potential corporate drone espionage before they even occur.

This Comment will argue that C-UAS technology is justifiable under the established self-help doctrine. Self-help is warranted as current trade secret law is inadequate to remedy damage done by espionage by drone, it would not substantially undermine law and order, and it is reasonable seeing as corporations could be held strictly liable for any wrong use of the technology. Additionally, there is much support for self-help in cyberspace, as networked computers and their systems are seen as property.[17] This Comment

---

[10] *See* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7, at 9.
[11] *See id.* at 9-10.
[12] *See id.* at 7-8.
[13] *See* discussion *infra* Section II.A.1.
[14] *See* discussion *infra* Section I.A.2.
[15] *See* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7, at 13.
[16] *See id.* at 13-15.
[17] *See* discussion *infra* Section II.B.1.c.

will also argue that the reasonable measures of protection standards under trade secret law and the Federal Trade Commission necessitate the use of C-UAS. Next, it will argue that espionage and cyber misappropriation conducted by drones create an economic imbalance that can only be equalized by C-UAS technology.

This Comment will also argue that an overhaul of the current statutory scheme in place is necessary in order for C-UAS technology to be adequately used by corporations. First, Congress needs to update the existing statutes in place that currently implicate C-UAS technology, as this was not the legislative intent behind the statutes.[18] Secondly, the Federal Aviation Administration must reclassify drones. The current classification of drones as "aircraft"[19] presents multiple problems that could easily be solved with this change and would allow for broader C-UAS use.

Lastly, this Comment will address several potential counter-arguments and concerns: 1) the issue of keeping C-UAS technology from bad actors can be solved by a licensing/authorization program administered by the U.S. Department of Justice ("DOJ"); 2) C-UAS technology can be mitigated by formal rules of engagement; 3) corporations must be responsible for their own C-UAS technology use as other programs will be insufficient; and 4) C-UAS technology has been successfully used in foreign countries and other American industries.

I. BACKGROUND

A. Traditional Corporate Espionage

In order to understand the role of drones in the espionage tactics of today, we must first understand traditional corporate espionage tactics. Corporate espionage has been a facet in business practices since the age of commerce began.[20] Corporate espionage is "the practice of using espionage techniques for commercial or

---

[18] *See* discussion *infra* Section II.C.1.

[19] *See* Huerta v. Pirker, N.T.S.B. Ord. No. EA-5730, 6-7 (Nov. 17, 2014), 2014 WL 8095629, at *3.

[20] Stone, *supra* note 1, at 8 ("For as long as there has been commerce, there has been espionage.").

financial purposes."[21] Some go as far as to say that "the theft of trade secrets has marked a transfer of power almost as routinely as bloodshed."[22] Arguably, one of the earliest instances of trade secret misappropriation involves the Byzantine empire and the Chinese Silk Road.[23] In more recent incidents, major corporations like General Motors, Gillette, Google, HP, Microsoft, and many more household names have fallen victim to corporate espionage.[24] As of 2004, "[m]ore than 50 percent of Fortune 1000 companies [admitted to having] been victims of corporate espionage," and at the time, it costed "American businesses approximately $200 billion annually."[25]

1. Traditional Espionage Tactics

Traditional espionage mirrors Cold War-style intelligence techniques.[26] Like in the Cold War era, today, we use the most recent and available technology. Recently, drones have been used in the War on Terror and are popular for anyone conducting a covert operation.[27] Sometimes, traditional corporate espionage tactics

---

[21] Fruhlinger, *supra* note 5.

[22] Mara Hvistendahl, *The Oldest Game: The Very Long History of Industrial Espionage*, FOREIGN POL'Y (Apr. 27, 2019), https://foreignpolicy.com/2019/04/27/the-oldest-game-industrial-espionage-timeline/ [https://perma.cc/Y3T5-ZLZM]. For an in-depth look into the United States' history with trade secret theft and its connection to our founding, see generally DORON S. BEN-ATAR, TRADE SECRETS: INTELLECTUAL PIRACY AND THE ORIGINS OF AMERICAN INDUSTRIAL POWER (2004). "Today, however, the United States is the one defending its position against other perpetrators . . . ." Hvistendahl, *supra*.

[23] *See* Hvistendahl, *supra* note 22 ("According to the Byzantine historian Procopius, Emperor Justinian sends Nestorian Christian monks to China to bring back the secret of silk. They return to Byzantium with silkworm eggs concealed in their staffs, which later hatch, breaking the Chinese monopoly."). For a timeline of instances where industries have been affected by trade secret theft, see generally *id.* Some other historical instances include the French stealing Chinese porcelain techniques, the American theft of British textile mills and looms, and the British espionage of Chinese tea. *See id.*

[24] *See Famous Cases of Corporate Espionage*, *supra* note 1.

[25] Rodgers & Marrs, *supra* note 3, at 62.

[26] *See* Santiago A. Cueto, *Spies, Lies and Secrets: 37 Industrial Espionage Tactics that Threaten to Kill Your International Business*, INT'L BUS. L. ADVISOR (Sept. 19, 2013), http://internationalbusinesslawadvisor.com/37-industrial-espionage-tactics-that-threaten-to-kill-your-international-business/ [https://perma.cc/7ZGW-LFN6].

[27] Lily Hamourtziadou, *Five Myths About Drone Warfare Busted*, CONVERSATION (Sept. 15, 2021, 10:18 AM), https://theconversation.com/five-myths-about-drone-warfare-busted-133660 [https://perma.cc/B45B-RRSZ]. *See also Companies and Data*

may still be more attractive than those conducted by hackers or with drones. The traditional tactics are much like one envisions when thinking of traditional spying. These include: theft, extortion, blackmail, mole planting, seduction, bribery, foreign intelligence recruits, communication interception, bogus interviews, wiretapping, and eavesdropping.[28] Threats can come from insiders and outsiders.[29] Usually, the biggest threat to companies in the realm of espionage is their employees, past or present, due to their access and ability to "steal documents, files, customer lists, and trade secrets."[30] Employees can be bribed to steal such information and sell it to the highest bidder.[31] There can also be external threats of espionage. Competitors and corporate recruiting agencies have also been common conductors of espionage.[32] Additionally, "[f]oreign governments often engage their own intelligence services to acquire trade or research secrets for their own national purposes or industries."[33] Other culprits may be "private investigative firms, hackers and thieves."[34]

2. Trade Secret Law

Trade secret misappropriation claims can be litigated under trade secret laws, though this is an unattractive and often

---

Centers Should Consider Drones When Assessing Security Risks, 911 SECURITY [hereinafter *Companies and Data Centers*], https://www.911security.com/blog/companies-and-data-centers-should-consider-drones-when-assessing-security-risks [https://perma.cc/HV3E-S7XK] (last visited Jan. 8, 2022).

[28] For a more exhaustive list, see Cueto, *supra* note 26 (also detailing computer, travel, and visitor espionage).

[29] *See* Mike Elgan, *10 Myths and Misconceptions About Industrial Espionage*, SEC. INTEL. (Nov. 8, 2019), https://securityintelligence.com/articles/10-myths-and-misconceptions-about-industrial-espionage/ [https://perma.cc/4SFD-N49B] (describing the top ten myths of corporate espionage in 2019).

[30] Cueto, *supra* note 26.

[31] *Id. See also* Rodgers & Marrs, *supra* note 3, at 62 ("[A]pproximately 85 percent of all corporate espionage incidents involve current or past employees.").

[32] Cueto, *supra* note 26 ("Competitors will often use recruiters to hire away employees of a target company for the sole purpose of collecting critical information.").

[33] *Id.* This is what is commonly referred to as "economic espionage." China is one of the biggest culprits of economic espionage. *See* Aarshi Tirkey & Harsh V. Pant, *China Faces a New Threat as US Cracks Down on Economic Espionage*, OBSERVER RSCH. FOUND. (Feb. 24, 2020), https://www.orfonline.org/research/china-faces-a-new-threat-as-us-cracks-down-on-economic-espionage-61612/ [https://perma.cc/L864-M2G2].

[34] Cueto, *supra* note 26.

expensive option.[35] Drones are used by bad actors because they are cheap, easily accessible, and challenging to detect, and there are few options regarding protection against them due to the current regulations.[36] This means that it is challenging to determine when a trade secret has been misappropriated. Like with hacking techniques, when a cyber trade secret is stolen, it is likely just copied—a company may never notice that it was stolen—but drones add another layer of complication with their remote-sensing capabilities. The bad actor does not even have to step foot inside of the building or data center to steal a trade secret. In order to understand why trade secret claims are less attractive than C-UAS proactive use when it comes to drones, we must first examine the basics of trade secret law.

"Trade secret law is [mostly] state law" adopted from three sources: the Uniform Trade Secrets Act ("UTSA"), the *Restatement (First) of Torts*, and the *Restatement (Third) of Unfair Competition*.[37] The federal laws that apply to trade secret protection are the Economic Espionage Act of 1996[38] and the Defend Trade Secrets Act of 2016.[39]

a. State Law

Every state has adopted its own trade secret law, with the UTSA being the most prominent source of authority.[40] The goal of the UTSA was "to create 'unitary definitions of trade secret and trade secret misappropriation,' as well as to codify basic principles

---

[35] *See* Jonathan E. Schulz, *Ex Parte Seizure Orders Under the Defend Trade Secrets Act: Guidance from the Courts During the Statute's First Year*, BRADLEY (June 26, 2017), https://www.bradley.com/insights/publications/2017/06/ex-parte-seizure-orders-under-the-defend-trade-secrets-act-guidance-from-the-courts [https://perma.cc/9G6K-TZEZ] (describing that litigants face an "uphill climb").

[36] *See* Stephen Pritchard, *Drones Are Quickly Becoming a Cybersecurity Nightmare*, THREATPOST (Mar. 22, 2019, 2:33 PM), https://threatpost.com/drones-breach-cyberdefenses/143075/ [Perma.cc link unavailable].

[37] *See* Jonathan Green, Comment, *Trade Secrets and Data Security: A Proposed Minimum Standard of Reasonable Data Security Efforts When Seeking Trade Secret Protection for Consumer Information*, 46 CUMB. L. REV. 181, 184 (2016).

[38] Pub. L. No. 104-294, 110 Stat. 3488 (codified as amended at 18 U.S.C. §§ 1831-1839).

[39] Pub. L. No. 114-153, 130 Stat. 376.

[40] *Id.* at 184-85 (forty-eight states have adopted the UTSA). This Comment will focus on the UTSA, rather than going into the particularities of each states' laws.

that had been developed through case law, thereby representing 'the first major attempt to legislate trade secret misappropriation.'"[41] The UTSA defines a "trade secret" as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[42]

Most states have adopted this language verbatim, and others have minor differences that do not affect the overall enforcement of trade secret protection.[43]

The *Restatement (First) of Torts* does not define trade secret, but states:

> A trade secret may consist of any formula, pattern, device of compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage of competitors who do not know or use it. . . . [I]t is not simply information as to a single or ephemeral events in the conduct of the business, as for example, the amount or other terms of a secret bid for a contract . . . . A trade secret is a process or device for continuous use in the operation of a [sic] business. . . .[44]

The *Restatement (First) of Torts* also provides a six-factor test to determine the existence of a trade secret:

---

[41] Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L.J. 829, 841 (2017) (footnotes omitted).

[42] Green, *supra* note 37, at 185 (alteration in original) (quoting UNIF. TRADE SECRETS ACT § 1(4) (UNIF. L. COMM'N 1985)).

[43] *Id.*

[44] *Id.* at 185-86 (alterations in original) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. L. INST. 1939)).

> (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[45]

Some courts look to the framework provided by the *Restatement (First) of Torts*, but the UTSA and the *Restatement (Third) of Unfair Competition* are the more modern and controlling authorities.[46]

The definition of a trade secret in the *Restatement (Third) of Unfair Competition* is: "[A]ny information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[47] This definition is different than the one provided in the UTSA.[48] The key differences between the Restatements and the UTSA are:

> First, the Restatements allow for a broader and more flexible approach when determining whether information is a trade secret than does the UTSA. Second, the more modern approach illustrated in the UTSA and the *Restatement of Unfair Competition* does not require continuous use by the owner. Third, the UTSA puts more emphasis on the proprietary holder's efforts to keep the information secret.[49]

In order to qualify for trade secret protection, the information must be secret, have value, be under reasonable efforts of protection, and be protectable information.[50] The UTSA defines secrecy as information that is neither "generally known" nor

---

[45] *Id.* at 186 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. L. INST. 1939)).

[46] *Id.*

[47] *Id.* (alteration in original) (quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (AM. L. INST. 1995)).

[48] *Id.* at 186-87.

[49] *Id.* at 187 (footnotes omitted).

[50] *Id.* at 187-201 (following the UTSA elements).

"readily ascertainable."[51] The reasonable measures of protection factor is arguably the most important factor in deciding whether the trade secret is granted legal protection.[52] Typically, courts look at the totality of the circumstances when determining the presence of reasonable efforts.[53] Other courts use a cost-benefit analysis to do so.[54] There is much discrepancy among courts as to what exactly qualifies as reasonable measures.[55]

In order to have a claim, not only must the above elements be met, but there must also be some sort of misappropriation of the trade secret. This occurs, under the UTSA, when there is "[a]cquisition of a trade secret through improper means, or improper disclosure of a trade secret."[56] "'Improper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[57]

b. Federal Laws

After the Cold War, Congress enacted the Economic Espionage Act of 1996 ("EEA").[58] The EEA "criminalizes the theft of trade secrets with the intent to benefit a foreign government."[59] Congress enacted the EEA because foreign enemies were utilizing their military spies to gain intelligence on the trade secrets of American

---

[51] *Id.* at 187 (quoting UNIF. TRADE SECRETS ACT § 1(4)(i) (UNIF. L. COMM'N 1985)).

[52] *See id.* at 188 (stating that evidence of reasonable measures of protection can also help establish that the information "was and is indeed secret").

[53] *Id.* at 191.

[54] *Id.*

[55] *Id.* at 192.

[56] John Villasenor, *Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur*, 43 AIPLA Q.J. 329, 337 (2015).

[57] UNIF. TRADE SECRETS ACT § 1(1) (UNIF. L. COMM'N 1985).

[58] Robin L. Kuntz, *How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets*, 28 BERKELEY TECH. L.J. 901, 901 (2013).

[59] *Id.* The EEA has been unsuccessful in its mission. *Id.* ("The EEA has largely failed in its purpose, and today, economic threats from abroad have grown even stronger. Between 2011 and 2012, economic espionage losses to the U.S. economy exceeded $13 billion."). This Comment will not provide an in-depth coverage of the EEA, as that law focuses mostly on economic espionage (i.e., foreign governments spying on other states or corporations) and was recently amended in 2016 by the Defend Trade Secrets Act. *See infra* text accompanying note 63. Though economic espionage does occur by drones and could be substituted for corporate espionage in this Comment, the UTSA and DTSA are better places to look for a general analysis.

businesses.[60] This was the first federal, and criminal, law involving trade secret protection; however, the EEA did not provide a civil claim of action.[61] The EEA defined "trade secret" as:

> [A]ny information that "(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) . . . derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." An owner for these purposes is one "in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed."[62]

The Defend Trade Secrets Act ("DTSA"), signed into law in 2016, amended the EEA and is the first law to provide a federal civil action for the misappropriation of trade secrets.[63] The DTSA does not preempt state trade secret laws, meaning that plaintiffs now have a choice of either state or federal courts to bring their misappropriation claims.[64] The DTSA broadened the definition of trade secret from the EEA to mean: "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."[65] "The DTSA also provides that information 'stored' only in an individual's memory" can be a trade secret in a misappropriation claim.[66] This brings the definition of trade secret

---

[60] Kuntz, *supra* note 58, at 901.

[61] *See id.* at 904-05.

[62] CHARLES DOYLE, CONG. RSCH. SERV., R42681, STEALING TRADE SECRETS AND ECONOMIC ESPIONAGE: AN OVERVIEW OF THE ECONOMIC ESPIONAGE ACT 3 (2016) (omission in original) (footnote omitted) (quoting 18 U.S.C. § 1839(3)-(4)).

[63] Peter J. Toren, *The Defend Trade Secrets Act*, INTELL. PROP. & TECH. L.J., July 2016, at 3, 3.

[64] *Id.*

[65] Orly Lobel, *The DTSA and the New Secrecy Ecology*, 1 BUS., ENTREPRENEURSHIP & TAX L. REV. 369, 371 (2017) (quoting Bret A. Cohen et al., *Explaining the Defend Trade Secrets Act*, A.B.A.: BUS. L. TODAY (Sept. 22, 2016), https://businesslawtoday.org/2016/09/explaining-the-defend-trade-secrets-act/ [https://perma.cc/Q576-CBLR]). This definition is broader than the UTSA's as well. *See supra* text accompanying note 42.

[66] Toren, *supra* note 63, at 4.

in the federal realm closer to that of the states following the UTSA.[67]

In order to qualify for trade secret protection under the DTSA, the information must meet the definition of a trade secret, and:

> (1) the information is actually secret, because it is neither known to, nor readily ascertainable by, another person who can obtain economic value from the disclosure or use of the information; (2) the owner has taken "reasonable measures" to maintain the secrecy; and (3) independent economic value is derived from that secrecy.[68]

Examining the "reasonable measures" element shows that the test focuses on the precautions taken by the owner to protect the secrecy of the trade secret and on the standards of that particular industry.[69] There is not a clear definition of "reasonable measures" provided in the DTSA, and courts are hesitant to provide one as well.[70] Generally, the rule is that "the more security measures that are instituted the more likely that a court will find that the sum total of such measures are reasonable."[71] Further, the owner of the trade secret "must assess the value of the material it seeks to protect, the extent of theft, and the ease of theft in determining how extensive their protective measures should be."[72] To put it simply, the owner must determine the value of the trade secret and then protect the secret in a reasonable manner in respect to that value.

Like the UTSA, for a DTSA trade secret claim to be successful, misappropriation of the trade secret must occur.[73]

> Misappropriation [of a trade secret] under the DTSA, in general, includes: without permission (A) obtaining a trade secret that was knowingly obtained through improper means or (B) disclosing or using a trade secret without knowing either

---

[67] *Id.* ("The *sine qua non* of an action under the DTSA is the existence of a 'trade secret,' and it slightly amends the definition of trade secrets from what was found in the EEA to bring the definition more in line with the USTA [sic].").

[68] *Id.*

[69] *Id.* at 5.

[70] *Id.* ("Congress intentionally did not define what constitutes a 'reasonable measure' under the EEA.").

[71] *Id.*

[72] *Id.* (quoting 142 CONG. REC. S12,213 (daily ed. Oct. 2, 1996)).

[73] *Id.* at 3-6.

> (1) that it is a trade secret or (2) that it was obtained through improper means.[74]

Misappropriation by "improper means" is a broad category, but the DTSA lists the following: "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[75] Furthermore,

> The terms "disclosure or use" means: a person—(i) used improper means to acquire knowledge of the trade secret; (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—(I) Derived from or through a person who used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii) before a material change of the position of the person, knew or had reason to know that—(I) the trade secret was a trade secret; and (II) knowledge of the trade secret had been acquired by accident or mistake.[76]

The key difference in the DTSA is that it allows for an ex parte seizure of the property containing the trade secret in certain, specific, circumstances.[77] There is no similar remedy under the UTSA or other state trade secret laws.[78] An ex parte seizure allows for the immediate dispatch of U.S. Marshalls to seize the stolen trade secret, without any opposition from the adverse party.[79] The seizure can be conducted "without advanced notice to the accused."[80] The purpose is "to prevent dissemination of the trade

---

[74] *Id.* at 5.

[75] *Id.* (quoting 18 U.S.C. § 1839(6)(A)).

[76] *Id.* (quoting 18 U.S.C. § 1839(5)(B)).

[77] *See id.* at 6-8.

[78] *See id.* at 6.

[79] *See The DTSA's Ex Parte Seizure Remedy – Two Years Later*, FISHER PHILLIPS (Aug. 7, 2018), https://www.fisherphillips.com/Non-Compete-and-Trade-Secrets/DTSA-ex-parte-seizure-remedy-two-years-later [https://perma.cc/6KJG-C4SC].

[80] Heather Bowen, *Cloud Computing Technology: Providing a Safer Way for Businesses to Protect Trade Secrets Under the Defend Trade Secrets Act*, 21 INTELL. PROP. & TECH. L.J. 79, 86-87 (2017).

secrets at issue."[81] There is a high burden to meet in order for this seizure to be granted and is only to be done in "extraordinary circumstances."[82] The burden has been described as an "uphill climb."[83] The seizure may not be ordered "'unless the court finds that it clearly appears from specific facts' that eight separate statutory requirements are satisfied."[84] Only a few litigants sought an ex parte seizure during the first year of its enactment, and most were unsuccessful.[85]

B. Advanced Corporate Espionage

1. Modern Espionage Tactics

As technology advances, so do espionage tactics. Hacking and cyberattacks are now another way that espionage can be carried out. Cybercrime is an attractive option as the perpetrators' identities can be hidden.[86] The use of technology to steal trade secrets is called cyber misappropriation.[87] Due to the advancement of technology, more trade secrets than ever are stored electronically.[88] This has facilitated the rise of cyberattacks and has "created a storm perfectly ripe" for espionage.[89] Just like traditional espionage, cyber misappropriation is prevalent in today's business world. "Companies are being attacked at least once a week," and "[c]yber criminals have stolen up to $1 trillion worth of intellectual

---

[81] *Id.* at 87.

[82] *Id.* (quoting 18 U.S.C. § 1836(b)(2)(A)(i)). Arguably, trade secret misappropriation by drone would qualify as an "extraordinary circumstance"; however, it is unclear whether the seizure of this property would violate the Aircraft Piracy Act. *See* 49 U.S.C. § 46502.

[83] Schulz, *supra* note 35.

[84] *Id.* (citing 18 U.S.C. § 1836(b)(2)(A)(ii)).

[85] *Id.*

[86] *See* Hanford, *supra* note 2, at 22 ("Criminals are difficult to find in cyberspace, because 'there is no equivalent of a DNA sample or fingerprint to identify the perpetrator of a specific cyber crime.' Perpetrators use proxy servers, virtual private networks, or peer-to-peer software to hide their identities within the vast world of cyberspace") (footnote omitted) (quoting DJ Summers, *Fighting in the Cyber Trenches*, FORTUNE (Oct. 13, 2014, 7:39 AM), https://fortune.com/2014/10/13/cold-war-on-business-cyber-warfare/ [https://perma.cc/DXL9-MSG5]). However, Hanford goes on to explain that there are still ways to find the perpetrators in some instances. *See id.*

[87] Elizabeth A. Rowe, *Rats, Traps, and Trade Secrets*, 57 B.C. L. REV. 381, 382 (2016).

[88] *See id.* at 381-82; Bowen, *supra* note 80, at 79-81.

[89] Rowe, *supra* note 87, at 382.

property in a single year."[90] According to a 2016 study, "a data center outage costs around $9,000 per minute," and "the average outage lasted 95 minutes."[91] However, it is difficult to accurately quantify this problem.[92] Companies may be "[un]aware that they have been victimized," and "[e]ven when discovered, there is no reliable method" for calculating the actual dollar value of the loss.[93] Some companies choose not to report the loss at all.[94] In 2012, Robert Mueller[95] posited, "[T]here are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[96]

Most recently, drones are now being used to conduct corporate espionage and cyberattacks.[97] Arguably, drones are the future of corporate espionage due to their ease of accessibility, undetectability, and relatively low cost.[98] This creates a novel problem for corporations. Drones allow a new medium for hackers as they are able to carry nefarious payloads to conduct cyber misappropriation, which allows for easier and more frequent hacking.[99] To put it into perspective, a bad actor could easily fly a drone over an office, hack into their wireless printer—stealing likely important documents—and then gain access to the office's

---

[90] *Id.* at 384.

[91] *Companies and Data Centers*, *supra* note 27. Drones can be used to physically cause outages as well by disabling heating and cooling systems of the building. *See id.*

[92] Rowe, *supra* note 87, at 385-86 ("The precise numbers and actual extent of economic espionage is difficult to ascertain.").

[93] *Id.* at 386.

[94] *See id.*

[95] Mueller was the FBI Director at the time. *Directors, Then and Now*, FBI, https://www.fbi.gov/history/directors [https://perma.cc/5MM7-CGSC] (last visited Jan. 8, 2022).

[96] Villasenor, *supra* note 56, at 330 (quoting Robert S. Mueller, III, Director, FBI, Speech at RSA Cyber Security Conference (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies [https://perma.cc/3THX-JQB2]). RedCurl, "[a] Russian-speaking hacking group specializing in corporate espionage[,] has carried out 26 campaigns since 2018 in attempts to steal vast amounts of data from the private sector." Jeff Stone, *An Advanced Group Specializing in Corporate Espionage Is on a Hacking Spree*, CYBERSCOOP (Aug. 13, 2020), https://www.cyberscoop.com/redcurl-groupib-russian-hacking-espionage/ [https://perma.cc/V95E-2UFK].

[97] *Companies and Data Centers*, *supra* note 27.

[98] *See* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7, at 6.

[99] *See id.* at 9.

internet system.[100] Drones, also referred to as Unmanned Aircraft Systems ("UAS"), are also attractive to corporate spies as "[e]ven the most physically fortified structures have a security gap when it comes to drones, the flying devices can easily penetrate their perimeter security controls."[101] Drones are capable of carrying malicious payloads, which hackers can use "to intercept or disrupt data communications or hack into servers."[102] Recently, researchers have shown that drones can easily bypass the once-impenetrable "'air gap' security safeguard."[103] Air gapped systems work by physically isolating a secure computer from unsecured networks, such as the internet or a local network.[104] Drones "can also be used in reconnaissance missions,"[105] as well as be utilized in traditional spying techniques.[106]

This is not a future threat—drones are being used for corporate espionage now. Companies like Apple, Facebook, and Tesla "have experienced public incidents of drones conducting aerial espionage," even after Apple "declared [its] campus a 'No Drone Zone.'"[107] The Louisiana Chemical Association has also faced incidents of "malicious, unauthorized activity" involving drones.[108]

---

[100] *See* Kelly Hodgkins, *This Smartphone-Equipped Drone Breaks into Wi-Fi Networks Through Unsecure Printers*, DIGIT. TRENDS (Oct. 6, 2015), https://www.digitaltrends.com/cool-tech/drone-hack-wireless-printer/ [https://perma.cc/W6WN-2EKT].

[101] *Companies and Data Centers*, *supra* note 27 ("Corporate spies and hackers are utilizing drone technology to steal trade secrets, confidential information, and other sensitive data from corporations and data centers.").

[102] *Id.* ("Wireless, Bluetooth, and RFID signals are all vulnerable to drone cyberattacks. Hacker drones can access signals a traditional off-site hacker could not obtain.").

[103] *Id.* ("[R]esearchers at Ben-Gurion's cybersecurity lab devised a method to penetrate the 'air gap' security safeguard.").

[104] Claudio Buttice, *Air Gap*, TECHOPEDIA, https://www.techopedia.com/definition/17037/air-gap [https://perma.cc/AER9-9QHG] (June 10, 2021).

[105] *Companies and Data Centers*, *supra* note 27 ("Drones can record who is coming and going from the building, identify patterns in security personnel units or other key employees.").

[106] *Id.* ("Drones can be used to peer in windows to record meetings, or to identify any valuable information in plain sight.").

[107] *Id.* ("If you want to know what the Tesla factory is up [sic], you can google Tesla factory drone footage and find a number of videos.").

[108] Sam Barnes, *Real and Present Danger: Industrial Plants Face a New Level of Threats from Drones, Cyberattacks and Corporate Espionage*, 1012 INDUS. REP. (May 4, 2020), https://www.1012industryreport.com/safety/real-and-present-danger-industrial-

Volke, a German automobile design corporation, "[d]iscovered espionage of their intellectual property by competitors using unauthorized drones" and have now taken steps to secure their airspace to prevent further espionage.[109]

2. Applicable Laws to Modern Tactics

a. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") is a federal law adopted specifically to fight computer hacking.[110] Though "it does not directly address trade secret misappropriation," there is a distinct overlap that arises in a claim of cyber misappropriation.[111] "The CFAA makes it a crime for anyone to intentionally access a computer without authorization, or surpass authorization, in order to access 'information from any protected computer.'"[112] This "principal wrongdoing" in CFAA "conceptually overlap[s] with the improper acquisition provisions of trade secret law."[113] Meaning that, "if the facts of a trade secret case involve the acquisition of trade secrets that are stored on a computer, the plaintiff in a civil trade secret case might also pursue a criminal prosecution under the CFAA."[114] Traditionally, prosecuting a claim under the EEA was difficult because "proof that the information stolen was a trade secret" and that the thief was conscious of that was required.[115] However, under CFAA, the burden of proof is lowered—all that

plants-face-a-new-level-of-threats-from-drones-cyberattacks-and-corporate-espionage/ [https://perma.cc/9ZEP-EL5L] ("We've seen indicators and evidence of foreign governments using drones equipped with high resolution video cameras and other types of photographic evidence at night . . . ."). Dow USA has also "detected drones flying within the boundaries of its facilities." *Id.*

[109] *Volke*, DEDRONE, https://www.dedrone.com/customers/volke [https://perma.cc/YT83-PDA6] (last visited Mar. 31, 2022).

[110] Rowe, *supra* note 87, at 390.

[111] *Id.*

[112] *Id.* (quoting 18 U.S.C. § 1030(a)(2)(C)).

[113] *Id.*

[114] *Id.*

[115] Hope Viner Samborn, *Move Over, James Bond: Modern Corporate Spying Tactics Are Subtle, yet Still Dangerous*, A.B.A. J., July 2004, at 24, 24.

must be proven is whether a computer was accessed without authorization.[116] Whether a trade secret was stolen is irrelevant.[117]

b. Federal Aviation Administration

Drones are regulated by the Federal Aviation Administration ("FAA") under 14 C.F.R. Part 107.[118] There are varying regulations for hobbyists versus commercial drone users. For hobbyists, the drone must be registered and marked with the registration number.[119] Also, the pilot must "carry proof of registration" with him, "[f]ly only for recreational purposes," "[f]ly at or below 400 feet" above the ground, obtain authorization before flying in controlled airspace, and remain "within the visual line of sight or [within the line of sight of an] observer who is . . . physically next to[] and in direct communication with" the pilot.[120] Lastly, the drone cannot be flown at night, unless the drone has lighting that allows the pilot to know its location and orientation at all times, fly over any person, or "interfere with emergency response . . . activities."[121]

Commercial operators may "fly for work or business" matters.[122] Commercial operators may obtain waivers for certain requirements, but essentially must follow similar rules.[123] The waivers available include, among others: "[o]peration from a moving vehicle or aircraft," daylight operation, visible line of sight operation, "[v]isual observer," "[o]peration of multiple small [UAS]," operation over people, and "[o]peration in certain airspace."[124]

---

[116] *Id.*

[117] *Id.*

[118] *See* 14 C.F.R. §§ 107.1-107.205.

[119] *Recreational Flyers & Modeler Community-Based Organizations*, FAA, https://www.faa.gov/uas/recreational_fliers/ [https://perma.cc/C3L8-W6PU] (Jan. 5, 2022, 11:37 AM).

[120] *Id.*

[121] *Id.*; 14 C.F.R. §§ 107.29, 107.39.

[122] *Certificated Remote Pilots Including Commercial Operators*, FAA [hereinafter *Certificated Remote Pilots*], https://www.faa.gov/uas/commercial_operators/ [https://perma.cc/F6TR-L276] (June 29, 2021, 9:44 AM).

[123] *See id. See also Summary of Small Unmanned Aircraft Rule (Part 107)*, FED. AVIATION ADMIN. (June 21, 2016), https://www.faa.gov/uas/media/Part_107_Summary.pdf [https://perma.cc/RP5B-ZX4M].

[124] *Certificated Remote Pilots*, *supra* note 122.

Pilots must complete an application to obtain a waiver.[125] They must also complete a knowledge test and register their drone with the FAA.[126]

II. ARGUMENT

A. Corporations Need a More Proactive Response Against Espionage by Drone

Corporations are left physically, and legally, defenseless from espionage and cyberattacks by drones. Bad actors are using drones as a medium to conduct their espionage and cyberattacks because they are cheap, relatively easy to use, and virtually undetectable, and thus, it is harder to prosecute those bad actors.[127] Drones allow for isolated systems to be hacked, allow the operator to remain hidden, and can be operated by the most novice of hackers.[128] Additionally, trade secret claims are insufficient in these instances because the bad act has already been done—the trade secret has already been lost. Companies are lacking a more proactive measure of protection from espionage and cyberattack by drones. Corporations are also physically defenseless against attacks by drones as the countermeasures they require are mostly illegal in the United States.[129] Those countermeasures being counter-drone technology, often called counter-unmanned aircraft systems ("C-UAS").[130] It is clear that the only way to truly protect one's trade secrets is to ensure that they are never stolen from the company. In the past, traditional security measures were adequate, but in today's rapidly evolving, technology-driven world, corporations can no longer rely solely on outdated security. Ultimately, C-UAS technology should be available to corporations to use for protection against espionage and cybercrime by drones. There is a clear gap in the current legal landscape that leaves corporations defenseless against drones. In order for C-UAS technology to be utilized by

---

[125] *See id. See also Summary of Small Unmanned Aircraft Rule (Part 107)*, *supra* note 123.

[126] *Certificated Remote Pilots*, *supra* note 122.

[127] *See* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7, at 6-8.

[128] *See id.* at 6-12.

[129] *See* discussion *infra* Section II.A.1.

[130] *See* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7, at 6.

corporations, an overhaul of the current statutory scheme is necessary. This involves regulations promulgated by both the FAA and the Federal Communications Commission ("FCC") to be amended.

1. Most C-UAS Technology Is Generally Illegal in the United States

Counter-drone technology is widely available across the globe, but most is illegal in the United States under several different statutory frameworks.[131] Congress gave exclusive authorization to "the Departments of Defense, Energy, Justice, and Homeland Security" to use such systems in limited situations, and the FAA has been authorized to conduct testing activities.[132] C-UAS technology is divided into two types: detection and mitigation.[133]

Detection involves the monitoring or tracking of a drone, usually by "detect[ing] the physical presence of [the drone] or signals sent to or from the [drone]."[134] Systems using radio frequency capabilities to do so are likely to "implicate the Pen/Trap Statute and Wiretap Act."[135] Section 2512 under Title 18 of the U.S. Code "prohibits the manufacture, assembly, possession, sale, advertisement, and distribution of [such] devices."[136] This means that C-UAS technology, specifically those that use radio frequency systems to interfere with the drone, are illegal to sell, manufacture, or even be advertised in the United States.

Mitigation capabilities are further categorized into "non-kinetic" and "kinetic."[137] "Non-kinetic solutions use non-physical measures to disrupt or disable UAS, including [radio frequency], WiFi, or Global Positioning System (GPS) jamming; spoofing;

---

[131] *See Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems*, FCC (Aug. 2020) [hereinafter *Advisory on the Application of Federal Laws*], https://docs.fcc.gov/public/attachments/DOC-366222A1.pdf [https://perma.cc/37Q8-JMK9]. Drones are under the jurisdiction of the FAA, DOJ, DHS, DOD, and FCC. *See id.*

[132] *Id.*

[133] *See id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

hacking techniques; and non-destructive directed energy weapons."[138] Such measures fall within the scope of the CFAA, the Interference with the Operation of a Satellite statute, and the Communication Lines, Stations, or Systems statute, as well as the statutes mentioned for the detection capabilities.[139] Kinetic solutions include measures capable of causing physical damage or disruption to disable the drone, "including nets, projectiles, and lasers."[140] Due to the drone's classification as an "aircraft" by the FAA,[141] kinetic, and possibly non-kinetic, interferences with the drone may implicate the Aircraft Sabotage Act and the Aircraft Piracy Act.[142] Additionally, there are several laws enforced by the FCC relating to the use of the radio frequency spectrum that disallow jamming.[143] Essentially, companies only have limited legal access to drone detectors.[144]

B. C-UAS Technology Should Be Allowed for Commercial Purchase by Businesses in the United States

Counter-drone technology should be allowed for purchase by U.S. businesses as it is justified for several reasons. First, the use of counter-drone technology is permissible self-help in response to an attack because (1) the current laws in place are inadequate to provide equitable judicial remedies, (2) there will not be a threat to peace, and (3) only reasonable actions will be taken against the attacking drone. Second, the courts' and Congress's unwillingness to provide a clear definition of "reasonable measures of protection" under the classification of trade secrets[145] provides a clear need for corporations to have the utmost protections for their trade secrets and their consumers' data under the Federal Trade Commission's

---

[138] *Id.*

[139] *Id.* (referring respectively to 18 U.S.C. §§ 1030, 1367, 1362).

[140] *Id.*

[141] *See* Huerta v. Pirker, N.T.S.B. Ord. No. EA-5730, 6-7 (Nov. 17, 2014), 2014 WL 8095629, at *3.

[142] *See Advisory on the Application of Federal Laws*, *supra* note 131.

[143] *See id.*

[144] *See* Jonathan Rupprecht, *7 Big Problems with Counter Drone Technology (Drone Jammers, Anti Drone Guns, Etc.)*, RUPPRECHT L. (Aug. 13, 2021), https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems/ [https://perma.cc/G5GF-UAPA].

[145] *See supra* text accompanying notes 69-72.

("FTC") regulations. Third, there are substantial economic reasons for the implementation of counter-drone technology into our corporate society. Drones now allow more trade secrets to be misappropriated at an easier and cheaper rate;[146] thus, corporations need to be able to protect themselves from all imminent threats.

1. C-UAS Is Permissible Self-Help

Self-help is an extrajudicial principle allowed in several criminal and civil instances.[147] "[I]t is a remedy exercised by individuals as an alternative to seeking state-sanctioned aid."[148] The leading definition of "self-help" is "legally permissible conduct that individuals undertake absent the compulsion of law and without the assistance of a government official in efforts to prevent or remedy a legal wrong."[149] Self-help is often acclaimed to be "an efficient, or at least potentially efficient, alternative to the slower, costlier, and more cumbersome civil justice system."[150] Scholars argue that self-help is the "most obvious recourse" for those wronged, and "one of the many . . . efficient strategies individuals can undertake to protect their entitlements."[151]

Self-help is justified by two factors.[152] "First, the law recognizes that the judicial remedies available may sometimes be inadequate, or self-help remedies superior."[153] "Second, the law recognizes that in certain circumstances the use of self-help will only minimally impair society's interest in law and order."[154] Essentially, self-help is a viable option when "[t]he law is willing to permit extrajudicial remedies of an actor's own making where a

---

[146] *See* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7, at 6.

[147] For a more exhaustive list, see generally Douglas Ivor Brandon et al., *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845 (1984).

[148] Zoë Sinel, *De-Ciphering Self-Help*, 67 U. TORONTO L.J. 31, 32 (2017).

[149] *Id.* (quoting Brandon et al., *supra* note 147, at 850).

[150] *Id.*

[151] *Id.* at 32-33 (quoting F.H. LAWSON, REMEDIES OF ENGLISH LAW 1 (2d ed. 1980)).

[152] A. Michael Froomkin & P. Zak Colangelo, *Self-Defense Against Robots and Drones*, 48 CONN. L. REV. 1, 9 (2015).

[153] *Id.*

[154] *Id.*

judicial remedy is inconvenient or unavailable, and where self-help does not strongly threaten a breach of the peace."[155]

The general question in self-help cases is reasonableness.[156] Under common law, "threats to persons may be met with proportionate counter-violence. But threats to property . . . cannot in the main justify harms to persons."[157] Property may be defended "only with such steps as society views as reasonably necessary."[158] Significant harms "may justify unique and severe self-help remedies."[159] In the instance of drones being used to steal trade secrets and consumer data, we face a problem that could be solved under self-help principles.

a. The Law Provides Inadequate Remedies

Firstly, the judicial remedies in these situations are inadequate. By the time a trade secret case has been litigated, the bad deed has already been done. The secret has already been stolen, likely copied and spread, and no longer holds any value to the original owner. Under the DTSA, courts may seize the trade secret from the perpetrator, but the burden that must be met to do so is significant.[160] Additionally, many corporations do not know they have been attacked until some time after the crime has occurred.[161] Not to mention that even bringing a claim or prosecuting the wrong-doer would be very difficult unless the perpetrator was apprehended during the act. That is the exact reason drones are used as the medium in these situations—they are virtually undetectable, and the pilot would be hard to locate.[162] Furthermore, waiting on law enforcement presents the same problem. The corporation does not have the time to wait, and law enforcement

---

[155] *Id.*

[156] *Id.* ("Common-law self-help doctrine generally boils down to a reasonableness standard.").

[157] *Id.* at 9-10 (footnote omitted).

[158] *Id.* at 10.

[159] *Id.* ("Thus, the key issue in mapping the scope of permissible self-help against robots will be defining the harm posed by a tortfeasing robot: the threat of limited harms justifies only limited self-help remedies, while great harms may justify unique and severe self-help remedies.").

[160] Schulz, *supra* note 35.

[161] Sometimes, it can be years before companies realize they have been the victim of corporate espionage. *See* Rowe, *supra* note 87, at 385-86.

[162] *See* Pritchard, *supra* note 36.

likely will not have the resources or sufficient knowledge to handle the problem.[163] Self-help by C-UAS would, without a doubt, be more beneficial than depending on the courts to handle trade secret misappropriation by drone after the fact.[164] All available legal avenues—trade secret law, cyber law, and trespass and privacy laws—are unable to provide an equitable solution to the problem of trade secret misappropriation by drone.

Even though the elements and concepts of trade secret law seem "straightforward," bringing forth a successful trade secret claim is problematic.[165] "Trade secret litigation is complicated and expensive."[166] It can be difficult to show a jury that "a trade secret exists, . . . that the misappropriation caused harm, and that the harm can be quantified in damages."[167] Additionally, like previously discussed, companies may not even know a trade secret has been stolen for quite some time. Emerging technology makes this problem even more complicated. Trade secret law only provides a reactive remedy,[168] whereas C-UAS technology is a proactive security measure.

The advancement in technology has "far outpaced the law," which brings about this very challenge.[169] Trade secrets, now more than ever, are stored electronically, which leads to the rise of cyber intrusions.[170] Offenders are now unknown and are using remote access tools (like drones) to steal trade secrets.[171] Due to the "recent revisions to our patent laws, many believe that trade secrets might be even more important than patents."[172] The theft of trade secrets

---

[163] *See id.*

[164] *See id.* However, this Comment is not arguing that self-help is appropriate for all trade secret misappropriation cases.

[165] *See* Andrew P. Valentine, *Trade Secret Litigation: Trade Secrets Protection Programs May Make or Break Your Case*, DLA PIPER (Oct. 2019), https://www.dlapiper.com/uk/global/insights/publications/2019/10/disputes-issue-1/trade-secrets-protection-programs-may-make-or-break-your-case/ [https://perma.cc/DAK2-SJKK].

[166] *Id.*

[167] *Id.*

[168] *See* discussion *supra* Section I.A.2.

[169] Rowe, *supra* note 87, at 383.

[170] *See id.* at 389.

[171] *Id.* at 383.

[172] *Id.* at 381. Once a patent is received, anyone is able to search the patent database to find details about that patent. *See Search for Patents*, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/patents/search [https://perma.cc/QA4A-7UBQ] (Feb. 1, 2022,

is on the rise due to technology.[173] Not only is the advancing misappropriation of trade secrets a problem, but also there are not any "effective judicial or legislative tools with which to address it."[174] The risks are everywhere, and the problem is a part of a bigger issue—cybersecurity.[175] Scholars define theft of trade secrets resulting from cyberattacks as "cyber misappropriation."[176] This situation "is intertwined with the national discourse on and rhetoric that accompanies cyberattacks, as well as the shortcomings of existing laws that govern trade secret misappropriation."[177] It is hard to bring even traditional trade secret claims (and unpopular to do so), and it is even harder to bring a trade secret claim by cyber misappropriation.[178]

The CFAA "was adopted . . . to address the problem of computer hacking, [but] it does not directly address trade secret misappropriation."[179] Traditional trade secret law "covers how we control, protect, acquire, and use information."[180] However, due to the modern advancement of electronically stored data and its "intangible nature of information," there are challenges in how it is

---

11:29 AM). This is not as attractive as trade secret protection since trade secrets remain secret.

[173] Rowe, *supra* note 87, at 381-82 ("We live in a world where the most sensitive proprietary information can be carried on a mobile device in one's pocket or stored without a device 'in the cloud.' Although technology has made it easy to store vast amounts of data constituting trade secret information electronically, the Internet and the rise of cyber intrusions into computer systems and networks have created a storm perfectly ripe for corporate espionage and trade secret misappropriation.") (footnote omitted).

[174] *Id.* at 382 (describing the problem as "urgent, elusive, and significant").

[175] *Id.* at 386 ("The reality is that risks are everywhere, whether they are malware-based attacks, intrusions on networks, potential attacks on mobile devices, or potential cloud-based attacks. Thoughtful consideration of this complex issue requires recognition of its place within the larger context of cybersecurity, where all kinds of information, from personal consumer information to military secrets, can be targeted.") (footnote omitted).

[176] *See, e.g.*, *id.* at 382.

[177] *Id.* at 386.

[178] *See generally* Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*, 16 YALE J.L. & TECH. 172 (2014).

[179] *See* Rowe, *supra* note 87, at 390 (explaining that sometimes, the CFAA can be used to criminally prosecute trade secret misappropriation if the trade secret was stored on a computer and accessed without authorization).

[180] *Id.* at 392.

regulated and controlled and how others use it.[181] In the past, trade secrets were protected with real property principles, but that is no longer a viable approach in the cyber world of today.[182] There is a need for better and "more effective mechanisms and tools, from both a legal and business perspective, to better protect our information."[183] Trade secret owners are "required to take reasonable efforts to protect their trade secrets, but in the age of cyber intrusions and relatively invisible theft of trade secrets, it is a practical reality that cannot be overlooked."[184] Companies must have the right to protect themselves until the law catches up with the times.

Furthermore, the current legal landscape is also too inept to provide corporations redress from cyber misappropriation. This includes cybersecurity law. Even though "[t]he United States continues to face persistent threats to public and private infrastructure from increasingly sophisticated and determined adversaries,"[185] our cybersecurity efforts are lacking. Scholars argue that it is "more urgent than ever for the nation to develop a whole-of-nation response" to cyber threats.[186] The current U.S. laws in place that apply to cybersecurity "are outdated—often decades old—and in many cases lack a common purpose to address the current cybersecurity threats."[187] It is unlikely that these laws will be adequately updated anytime soon.[188] Congress is "out of touch with technology," and it is hard to say "whether lawmakers and their staffers have an adequate grasp of the challenges and potential solutions."[189] The April 2018 hearing on Facebook's privacy practices is demonstrative.[190] The lack of understanding of

---

[181] *Id.* at 392-93.

[182] *Id.* ("With real property[,] we can build fences, use locks, and attach alarms. Traditionally, that was the model that we used and developed to protect trade secrets. A new day has come, however, and that model may not serve as well going forward.") (footnote omitted).

[183] *Id.* at 393.

[184] *Id.* at 396.

[185] Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 812.

[186] *Id.*

[187] *Id.* at 813.

[188] *See id.* at 819-20.

[189] *Id.* at 820.

[190] *See id.* ("Unfortunately, recent events call into question whether lawmakers and their staffers have an adequate grasp of the challenges and potential solutions. Perhaps

the "basic mechanics" of the most commonly used Internet features "demonstrate[s] a far deeper problem with the ability of Washington to develop effective rules for technology companies."[191] Kosseff asks, "If members of Congress are unable to understand the basic business model and data flow for a two billion-member social media site, how are they expected to develop effective and enduring laws that will improve the cybersecurity of social media and other technology?"[192] There are "ever-increasing" threats, and "there is an urgent need for our laws to keep up."[193] It is clear that the cybersecurity laws currently in place are insufficient to protect corporations from cyber espionage.

Lastly, as for trespass and privacy laws, the FAA has left their enactment regarding drones to the states.[194] However, very few states have actually taken the steps to do so.[195] Even in the states that have, the classification of drones as aircraft raises several problems in enforcing such laws.[196] Courts must analyze drone trespassing issues as they would any aircraft, which typically means that unless the drone is disturbing the air the owner "enjoys," then it is not trespassing.[197] This issue illuminates the overall argument that drones should be classified as something other than aircraft and shows that traditional tort, or even

---

at no time was this clearer than April 2018, when the Senate Judiciary and Commerce Committees held a joint hearing on Facebook's privacy practices. For instance, Sen. Orrin Hatch asked Facebook CEO Mark Zuckerberg, 'How do you sustain a business model in which users don't pay for your service?' 'Senator, we run ads,' Zuckerberg responded.") (footnote omitted).

191 *Id.* ("Writing about the hearing for Vox, Emily Stewart observed that '[s]ome of the lines of questioning senators from both parties pursued demonstrated they aren't exactly the most tech-savvy bunch, aren't entirely clear on how Facebook works, or maybe have just never used the platform.' Sean Burch, writing in The Wrap, posited that 'Orrin Hatch might not have the best understanding of Facebook.' Jessica Rosenworcel, a commissioner on the Federal Communications Commission, wrote that the hearings 'made clear both how powerful new technologies are, and how important it is to have a common understanding of their basic mechanics.'") (alteration in original) (footnotes omitted).

192 *Id.*

193 *Id.* at 822 ("Every day, cybersecurity researchers spot new trends in threats from around the globe.").

194 Lane Page, Note, *Drone Trespass and the Line Separating the National Airspace and Private Property*, 86 GEO. WASH. L. REV. 1152, 1155, 1159 (2018).

195 *Id.* at 1165-67.

196 *See id.* at 1165.

197 *See id.* at 1164.

criminal, laws are incapable of handling claims involving drones.[198] The statutory and legal precedent in place does not provide a just opportunity for proper restitution from drone trespass or privacy violations. Corporations should be entitled to self-help.

b. C-UAS Will Not Undermine Law and Order

The remaining principle in permissible self-help circumstances is that it must not affect law and order. In this specific situation, the use of self-help by C-UAS would not substantially undermine society's interest in law and order. Corporations would only be taking action against those who are attacking them. This, in no way, would threaten a breach of the peace. By following set rules of engagement[199] and abiding by the traditional reasonableness standard of self-help,[200] companies would only need to take action when absolutely necessary. There is a minimal danger to society as C-UAS technology only involves the destruction of property and, likely, only in extreme circumstances. Corporations will not be jamming every drone that flies over their airspace. They will only be taking the appropriate reasonable measure in each specific circumstance. Additionally, the risk is low because if a corporation was to destroy a falsely identified, friendly drone, it would simply pay for the damages caused.

Corporations cannot depend on law enforcement in these situations. They are time sensitive, and waiting on police to arrive could be the difference between losing valuable trade secrets and consumer data, or keeping them secure. It is also unlikely that law enforcement would have the resources to properly handle the situation.[201]

c. Corporations Will Be Liable for Unreasonable Actions

The biggest question in self-help cases is reasonableness.[202] The actions taken against the criminal, trespasser, tortfeasor, etc.

---

[198] *See id.* at 1163-67.

[199] *See infra* Section III.A.

[200] *See supra* text accompanying notes 156-159.

[201] At the time of this Comment, individual law enforcement offices do not have authorization for C-UAS technology. *See Advisory on the Application of Federal Laws*, *supra* note 131.

[202] *See* Froomkin & Colangelo, *supra* note 152, at 9-10.

must be reasonable under the scope of the bad actor's engagements.[203] Under tort and criminal law, defense of self is justified, but it must be reasonable.[204] In this circumstance, however, the cyber misappropriation of trade secrets is a significant harm that necessitates unique counter measures of self-help. The designation of drones as property allows reasonable actions to be taken by corporations with C-UAS technology. Additionally, C-UAS technology allows for adequate protection of the corporation's property without any threat of harm to humans. This is a unique circumstance being as it is property versus property, and therefore, there is minimal risks to endangering human life. Trade secrets and networked computers have been defined as property,[205] and there is support for self-help in the realm of cyberspace.[206] It is not a great leap to apply those supported self-help principles to the protection of trade secrets with C-UAS technology.

Scholars have previously discussed the use of self-help in cyberspace.[207] Networked computers have been described as "a new form of chattel."[208] In *Register.com, Inc. v. Verio, Inc.*,[209] the Second Circuit held that computer systems were a form of property and allowed the plaintiff's trespass of chattels claim to be heard.[210] It would not be a substantial leap to define trade secrets, especially those stored on computer systems, or data as chattel.[211] This is not

---

[203] *See id.*

[204] *See id.*

[205] Trade secrets are a form of property, and as such, they are entitled to be protected. The U.S. Supreme Court in *Ruckelshaus v. Monsanto Co.* identified trade secrets as property. 467 U.S. 986, 1001-04 (1984). *See also* Argento, *supra* note 178, at 183 ("The Supreme Court, in particular, identified trade secrets as a form of property in *Ruckelshaus v. Monsanto*, rejecting its earlier view that trade secret rights rested purely on a commercial morality justification. Commentators and several state courts have also accepted this view.") (footnote omitted); Green, *supra* note 37, at 184 ("Due to the fungible nature of trade secrets, they are often treated as a form of property. Trade secrets are often sold, bought, licensed, and protected just as other tangible forms of property.") (footnote omitted).

[206] *See, e.g.*, Richard A. Epstein, *The Theory and Practice of Self-Help*, 1 J.L., ECON. & POL'Y 1, 30-31 (2005).

[207] *See id.*

[208] Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L., ECON. & POL'Y 171, 187 (2005) (quoting Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 76 (2003)).

[209] 356 F.3d 393 (2d Cir. 2004).

[210] Smith, *supra* note 208, at 188.

[211] *See id.* at 189.

to say that a trespass to chattels claim might be more successful, or even a viable option, in courts, but this allows "conceptualizing unauthorized access to computer systems as a tortious harm to 'property' . . . [and] thinking about such harms as property-related harms may provide such companies with latitude to engage in meaningful forms of self-help."[212] "[P]ossessors of chattels retain the 'privilege to use reasonable force' to protect their possessions—even against those 'harmless' interferences for which a formal legal action would be unavailing."[213] The *Restatement of Torts*:

> permits property owners to engage in forceful self-help—provided the intrusion is not "privileged," the property owner "reasonably believes that the intrusion can be prevented or terminated only by the force used," and the property owner "has first requested the other to desist and the other has disregarded the request, or the actor reasonably believes that a request will be useless or that substantial harm will be done before it can be made."[214]

Additionally, the *Restatement*:

> authorizes the use of "mechanical devices not threatening death or serious bodily harm" to protect land or chattels "from intrusion" if the use of the device is "reasonably necessary to protect the . . . chattels from intrusion," the use is "reasonable under the circumstances," and "the device is one customarily used for such a purpose, or reasonable care is taken to make its use known to probable intruders."[215]

By defining computer systems and data as property, corporations should be allowed to defend their property with C-UAS technology.[216]

---

[212] *Id.* (emphasis omitted).

[213] *Id.* at 190 (quoting RESTATEMENT (SECOND) OF TORTS § 218 cmt. e (AM. L. INST. 1965)).

[214] *Id.* (quoting RESTATEMENT (SECOND) OF TORTS § 77 (AM. L. INST. 1965)).

[215] *Id.* (alteration in original) (quoting RESTATEMENT (SECOND) OF TORTS § 84 (AM. L. INST. 1965)).

[216] *See id.* at 194-95 ("In this regard, the area of computer security resembles other areas of American law—ranging from repossession, to bail enforcement, to self-defense against threats of immediate bodily harm—where self-help measures remain important. Indeed, our current legal climate in the area of computer security bears certain resemblances to other contexts in which self-help has historically proved appealing,

2. Reasonable Measures of Protection Standard Necessitates C-UAS Technology

The law is clear under both the federal and state trade secret classification analyses. In order to gain trade secret classification, the secret must be under reasonable measures of protection as an effort to shield its secrecy.[217] As already discussed, the ambiguity of the reasonable-measures-of-protection standard is clear,[218] but this ambiguity necessitates the use of counter-drone technology by American businesses. The reasonable-measures-of-protection standard is the threshold to whether the legal protection of the stolen information as a trade secret is granted,[219] and thus, until there is a clear, uniform standard, corporations should be entitled to protect their trade secrets with justifiable security measures to ensure their protection. The FTC has a similar regulation for the protection of consumer data and a similar ambiguity of the required measures of protection necessary.[220] These requirements under established trade secret law and the FTC really seem to require C-UAS technology in order to combat advancing methods of misappropriation.

Counter-drone technology is reasonable when viewed from this light. It is relatively cheap, there are several defense options, and

---

including 'frontier' settings where formal legal systems were underdeveloped or non-existent, instances where formal law proved incapable of providing adequate or affordable remedies, and circumstances where potential offenders have proven to be indifferent to the effects of formal legal sanctions.") (footnotes omitted). *See also* Epstein, *supra* note 206, at 30 ("The inability to get powerful state remedies thus puts the emphasis back on the self-help remedies. In dealing with self-help, it is important not to lose sight of the fact that most users of the Internet happily avoid the use of any of these dubious techniques. But the problem is so intractable because it takes only a small group of anonymous individuals to disrupt the operation of the entire system.") (emphasis omitted); Rowe, *supra* note 87, at 383 ("Effectively addressing cyber misappropriation requires a holistic approach that must involve self-help on the part of trade secret holders. Reliance on the government, law enforcement, criminal laws, and other legal and judicial remedies have not been successful, and it is unlikely that, standing alone, they ever will be.").

[217] Toren, *supra* note 63, at 5.

[218] *See supra* text accompanying notes 69-72.

[219] *See* Esha Bandyopadhyay, *Safeguarding Secrecy: Taking "Reasonable" Measures to Protect Trade Secrets*, FISH & RICHARDSON (June 12, 2020), https://www.fr.com/safeguarding-secrecy-taking-reasonable-measures/ [https://perma.cc/827B-2FDF].

[220] *See* Green, *supra* note 37, at 204-05.

it is not super sophisticated.[221] Most C-UAS manufacturers and companies install the technology for you, conduct several demonstrations, and offer other support options,[222] meaning that overall, C-UAS technology would be rather easy to acquire and easy to use. When combined with a potential licensing program, set rules of engagement, and strict liability policies,[223] C-UAS technology becomes a more-than-reasonable measure of protection for corporations and their trade secrets.

a. Trade Secret Law Requires C-UAS

Traditional trade secret law is an inadequate pathway to restitution in today's technological world.[224] One of the main issues in any trade secret action is whether the company took reasonable steps to protect the trade secret.[225] In *E.I. duPont deNemours & Co. v. Christopher*,[226] the Fifth Circuit "analyzed a trade secret case involving aerial photography of an industrial plant owned by the plaintiff."[227] DuPont was in the process of constructing a plant to produce methanol in a secret manner.[228] The defendants relied on the fact they were in public airspace to support that it was not possible for them to have misappropriated the alleged trade secret.[229] They also argued that DuPont "did not take reasonable precautions in its failure to cover the facility during construction and thus allowed the facility to be viewed from the air."[230] The court refused that argument, holding "that it would be unfair to permit espionage 'when the protections required to prevent another's spying cost so much that the spirit of inventiveness is

---

[221] *See generally* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7.

[222] *See generally The Counter UAS Directory*, UNMANNED AIRSPACE (Feb. 2021), https://www.unmannedairspace.info/wp-content/uploads/2021/02/Counter-UAS-directory.-February-2021.v1.pdf [https://perma.cc/7EBA-DNLC].

[223] *See infra* Section III.A.

[224] The Uniform Trade Secrets Act has not been updated since 1985. *See* Sandeen & Seaman, *supra* note 41, at 841.

[225] Rodgers & Marrs, *supra* note 3, at 62.

[226] 431 F.2d 1012 (5th Cir. 1970).

[227] Victoria Schwartz, *Overcoming the Public-Private Divide in Privacy Analogies*, 67 HASTINGS L.J. 143, 154 (2015).

[228] *Id.*

[229] *Id.*

[230] *Id.* at 155.

dampened.'"[231] It further "explained that a trade secret owner should not be forced to 'guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available.'"[232] Again, this case is severely outdated seeing as it was heard in 1970,[233] but the holding may still be timely. We have reached a point where aerial trespass is anticipated, it is detectable, and it is preventable if C-UAS technology is available to corporations. In the *Christopher* case, valuable trade secrets were lost simply by the photographs taken by the defendants.[234] Imagine if a drone was used instead.

b. The FTC Requires C-UAS

Additionally, corporations have a duty to "institute programs and procedures designed to secure data collection, storage, handling, transport, and disposal."[235] Companies are not just storing their own information; they are storing their consumer's information, which must be protected. Procedures recommended by the FTC include "installing proper and current antivirus and anti-spying programs on computers within the network, creating procedures to assess security warnings and intrusion alerts, and maintaining and reviewing logs on network activity."[236] Scholars have argued that "when trade secrets involve consumer information, business should be required to protect that information at heightened levels of security and courts should not afford remedy or protection if those standards are not met."[237] Seeing as not only are the companies' trade secrets in danger, but also the consumers' data, corporations should have the means to adequately protect their data.

---

[231] *Id.* (quoting *Christopher*, 431 F.2d at 1016).
[232] *Id.* (quoting *Christopher*, 431 F.2d at 1016).
[233] *See Christopher*, 431 F.2d at 1012.
[234] *See id.* at 1013.
[235] Green, *supra* note 37, at 205.
[236] *Id.* at 208 (footnotes omitted).
[237] *Id.* at 218.

3. Trade Secret Misappropriation by Drone Creates an Economic Imbalance

Trade secrets are important to the American economy due to their influence on innovation and competition within markets.[238] Companies spend significant amounts of money to develop their trade secrets and then on protecting those trade secrets.[239] However, trade secrets, now more than ever, are stored electronically.[240] Our technological advancements and dependency on cloud-based networks have put those trade secrets and, in turn, our economy at risk.[241] Corporations are unable to fully protect their trade secrets from traditional and cyber misappropriation conducted by drones, and they are less willing to develop trade secrets if they can no longer adequately protect them.[242] Additionally, access to drones has broadened the types of trade secrets that are targeted.[243] Drones allow for more, and cheaper, trade secrets to be stolen.[244] This has created an imbalance because now, all trade secrets are at risk rather than those only seen as valuable enough to steal.[245] Drones bring the cost of the theft down, and now, bad actors are stealing more trade secrets.[246]

Trade secrets have always been important to the American economy, and now, technology has affected the overall role of those trade secrets.[247] Technology has had a major impact on the American workforce and has pushed the American economy to revolve around informational assets.[248] Trade secrets have become more important than ever to the economy:

> Consider the total value of the 500 companies, most of them publicly held, that constitute the S&P 500. Cornerstone

---

[238] *See generally* David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091 (2012).

[239] *See id.* at 1104-06.

[240] *See* Bowen, *supra* note 80, at 81-83.

[241] *See id.* at 84.

[242] *See generally* Argento, *supra* note 178; Rowe, *supra* note 87.

[243] *See* Robert A. Hazel, *Privacy and Trade Secret Law Applied to Drones: An Economic Analysis*, 19 COLUM. SCI. & TECH. L. REV. 340, 371 (2018).

[244] *See id.*

[245] *See id.*

[246] *See id.*

[247] *See generally* Almeling, *supra* note 238.

[248] *See id.* at 1098-1106.

> Research has found that in 1975, 17 percent of the total value of the S&P 500 consisted of intangible assets, which encompasses trade secrets and other forms of IP; by 2009, the value had grown to 81 percent.[249]

Trade secrets may now be more valuable than patents as well.[250] "[C]ompanies . . . rely on trade secrets to protect their competitive advantage."[251] Corporations spend a substantial amount of time and money to develop and research their trade secrets.[252] Due to this fact, the protection of trade secrets is of the utmost importance to their owners.[253] Corporations "thrive on making large initial investments of time and capital to develop information, formulas, designs, and products that enable them to subsequently recover the outlays in the marketplace."[254] Companies will only take risks developing such information if they are sure "that none of their competitors will be able to easily duplicate their efforts with a few strokes of the key."[255] "[O]ur economy depends heavily on vigorous competition between private companies, worker mobility, and follow-on innovation."[256]

Additionally, the importance of trade secrets is illustrated by the rise of trade secret litigation.[257] Litigation in federal courts doubled between 1995 and 2004.[258] "[L]itigation in state courts has also grown at a steady rate."[259] Due to "the high cost of trade secret litigation," this "suggest[s] that trade secrets are increasingly important to companies."[260] Macro trends predict that misappropriation of trade secrets will only increase, with the frontrunner being cyber misappropriation.[261]

---

[249] *Id.* at 1104.

[250] *See* Rowe, *supra* note 87, at 381.

[251] Argento, *supra* note 178, at 191.

[252] *See id.* at 183.

[253] *See id.*

[254] Gerald O'Hara, Comment, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS: J. COMMC'NS L. & POL'Y 241, 273 (2010).

[255] *Id.*

[256] Argento, *supra* note 178, at 235.

[257] *Id.* at 190-91.

[258] *Id.* at 191.

[259] *Id.*

[260] *Id.*

[261] *Id.* at 190.

Drones have now provided greater access to trade secrets and greater ease to steal them.[262] Information is now stored on cloud-based networks, meaning that information is more susceptible to hacking and misappropriation.[263] The addition of drones into this equation creates a problem that can only be solved by self-help. Drones can be utilized in all parts of a cyberattack—recon, data breaches, data center outages, etc. Drones are also an economically efficient choice for cyber misappropriation and cyberattacks.[264] At the time of the *Christopher* case, the defendants went to great lengths, at a great cost, to obtain the trade secret,[265] so we can assume that the secret was worth just as much. Today, however, drones are easily accessible, relatively cheap, and easily equipped with espionage and hacking tools,[266] meaning that bad actors do not have to go to such great lengths to obtain trade secrets. This implies that more trade secrets will be worth obtaining because it is cheaper and easier to do so.[267] In order to combat this, companies should have access to a drone defense system to meet the standard that they have adequately protected their trade secrets. C-UAS technology can help to provide a sense of homeostasis to the current economic imbalance created by trade secret misappropriation by drones.

C. An Overhaul of the Current Statutory Scheme Is Required

In order for C-UAS technology to be available for corporations to purchase and use legally to protect themselves from trade secret misappropriation by drone, either an authorization or licensing

---

[262] *See* Hazel, *supra* note 243, at 371.

[263] *See* Bowen, *supra* note 80, at 81-84.

[264] *See* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7, at 6.

[265] *See* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013-14 (5th Cir. 1970).

[266] *See generally* NAT'L URB. SEC. TECH. LAB'Y, *supra* note 7.

[267] *See* Hazel, *supra* note 243, at 369-71 ("What constitutes a reasonable precaution will vary with the value of the secret. A trade secret of high value, such as the formula for Coca Cola, should be, and is, closely guarded. A trade secret of low value, such as the client list for a small accounting firm, warrants only minimal protection. Similarly, those who seek to appropriate a trade secret will invest an amount based on their expected likelihood of success and the value of the trade secret. . . . However, because drones are far less expensive to acquire and operate, thieves can afford to launch many more surveillance flights and therefore are more likely to uncover secrets that are visible or detectable by drones.") (footnotes omitted).

procedure will need to be instituted, or Congress and the FAA must amend the laws currently in place prohibiting the use of C-UAS technology. This Comment will focus on the current implication of C-UAS technology under the Wiretap Act. Additionally, it will discuss the need for drones to be reclassified as something other than aircraft.

1. Statutes Should Not Implicate C-UAS

As listed earlier in this Comment, the use of C-UAS technology likely implicates several federal statutes. The largest implication arises under the Wiretap Act, which is where this Comment will focus. The Wiretap Act was originally promulgated to protect American citizens' Fourth Amendment rights from law enforcement.[268] It is clear that the Wiretap Act's scope is extended too far when implied to counter-drone technology as the original purpose does not align with its current use.

The Wiretap Act prohibits any person from "'intentionally intercept[ing]' the content of 'any . . . electronic communication[,]' unless it is conducted pursuant to a court order or a statutory exception applies."[269] The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[270] There is an exception for the "interception of electronic communications that are 'readily accessible to the general public.'"[271]

---

[268] *See Electronic Communications Privacy Act (ECPA)*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/ecpa/ [https://perma.cc/A477-6TCG] (last visited Jan. 8, 2022).

[269] *Advisory on the Application of Federal Laws*, *supra* note 131 (alterations in original) (quoting 18 U.S.C. § 2511). "Private actors are unable to obtain a court order under the Pen/Trap Statute and, therefore, must operate pursuant to one of the statute's exceptions." *Id.* at n.5. See also Helen Jazzar, Note, *Bringing an End to the Wiretap Act as Data Privacy Legislation*, 70 CASE W. RSRV. L. REV. 457 (2019), for an in-depth look at the Wiretap Act and its history.

[270] *Advisory on the Application of Federal Laws*, *supra* note 131 (quoting 18 U.S.C. § 2510(12)).

[271] *Id.* Those radio communications that do not fall into the exception are listed in Section 2510(16). *See* 18 U.S.C. § 2510(16). There is also an exception for "interception of any radio communications that are transmitted 'by any . . . aeronautical communications system.'" *Id.* (alteration in original) (quoting 18 U.S.C. §

The Wiretap Act was originally part of the Omnibus Crime Control and Safe Streets Act of 1968,[272] which was superseded by the Electronic Communications Privacy Act of 1986.[273] In 1968, its purpose was to "prevent crime and to insure the greater safety of the people."[274] In 1986, the Wiretap Act was amended to "grant[] law enforcement access to 'electronic communications,'" as described above.[275] At that time, Congress also "added a liability exemption for [electronic communications service providers ("ECSPs")]: the 'ordinary course of business' exception."[276] This "exception exempts an ECSP from liability for interceptions that occur 'in the ordinary course of its business.'"[277] Congress realized that "[t]he provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain."[278] Today, ECSPs are using the ordinary course of business exception to shield themselves from liability stemming from digital-targeted advertisements, and courts have allowed this because the exception is so ambiguous.[279] Though this does not apply specifically to the issue this Comment discusses, it is illustrative of

---

2511(2)(g)(ii)(IV)). "UAS [radio frequency] systems may be considered [as such] under the [Wiretap] Act. . . . [E]xisting case law raises questions as to the scope of both exceptions." *Id. See also* Joffe v. Google, Inc., 746 F.3d 920, 928-29 (9th Cir. 2013), *cert. denied*, 573 U.S. 947 (2014).

[272] Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2520).

[273] Pub. L. No. 99-508, 100 Stat. 1848.

[274] Omnibus Crime Control and Safe Streets Act, 82 Stat. at 197.

[275] Jazzar, *supra* note 269, at 461. Jazzar's Note focuses on the improper use of the Wiretap Act in deciding data privacy issues, specifically those using "digital users' information to create online-targeted advertisements." *Id.* at 462. That particular issue is beyond the scope of this Comment, but it illustrates the innate problems of the outdated Wiretap Act being used as data privacy legislation today.

[276] *Id.* at 461 (footnote omitted).

[277] *Id.* (quoting 18 U.S.C. § 2510(5)).

[278] S. REP. NO. 99-541, at 20 (1986). ECSPs involved in targeted-digital advertisements have used this exception to shield themselves from liability, though "the Wiretap Act's text suggests that the Act does not apply to digital marketing practices at all." Jazzar, *supra* note 269, at 469. Jazzar uses the differences between "an electronic communication and online behavior, and between device and software" to support this claim. *Id.* at 470.

[279] *See generally* Jazzar, *supra* note 269.

the Wiretap Act's overuse in areas it was not originally created to command.[280]

The definition of "electronic communication," some argue, is overextended when applied to "a transfer that does not involve a human on the receiving end of the communication."[281] The statutory language suggests "that a human has to be on the receiving end of an electronic communication" in order to fall within the Wiretap Act's scope.[282] Following this idea, "[i]t is significant that the Wiretap Act excludes from the definition of electronic communication any communication made through a 'tone-only paging device' or from a 'tracking device' because both . . . involve a 'transfer' between two devices that does not involve a human on its receiving end."[283] Additionally, the language used suggests that an electronic communication requires "at least two 'parties,' or [actual] individuals, involved."[284] This can be applied to drones and C-UAS technology. In that situation, no humans are involved, only computers. Thus, the Wiretap Act should not be implicated by using C-UAS technology.

Simply put, the Wiretap Act was not created to control the use of C-UAS technology. It was enacted to protect people's privacy in their conversations.[285] In general, the Wiretap Act prohibits electronic eavesdropping.[286] The Wiretap Act is severely outdated and, therefore, ambiguous as to what technologies it should actually apply.[287] Essentially, the statutes that are implicated by

---

[280] *See id.* at 458 ("Courts should not interpret the Wiretap Act to include conduct it was never intended to encompass.").

[281] *Id.* at 470.

[282] *Id.*

[283] *Id.*

[284] *Id.* at 470-71 ("The Wiretap Act generally 'protects the parties to a communication against the unlawful interception, use, and disclosure of that communication by persons who are not parties to the communication.' The Wiretap Act also allows an 'aggrieved person' to move to suppress the contents of an unlawfully intercepted communication. An 'aggrieved person' is any 'person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.'") (emphasis omitted) (footnotes omitted) (quoting United States v. Reed, 575 F.3d 900, 916 (9th Cir. 2009)).

[285] *See Electronic Communications Privacy Act (ECPA)*, *supra* note 268.

[286] *See* Jazzar, *supra* note 269, at 470-71.

[287] *See id.* at 459 ("The Wiretap Act was last amended at a time when the World Wide Web did not exist . . . .").

the use of C-UAS technology are ambiguous and applied improperly.

2. The FAA Should Reclassify Drones

Additionally, the FAA must reclassify drones as something other than aircraft. This is perhaps the biggest challenge corporations face in terms of drone defense as they are left remotely defenseless until after a bad act has already occurred. Seeing as a drone is classified as an aircraft and, therefore, illegal to shoot down, tamper with, or damage today,[288] if a company was to see a drone that it strongly suspected was up to no good, its only option would be to call the police, who would also be virtually unhelpful.[289]

The term "aircraft" is simply inappropriate for drones.[290] Drones and planes are not the same thing and, therefore, should not be classified under the same name. The most obvious difference is in their size and capabilities. Drones are much smaller than manned aerial vehicles, cannot fly at high altitudes, and do not carry passengers.[291] The classification of drones as aircrafts has placed a significant burden on their regulation rather than alleviating the problems that arise out of drone use.[292] The FAA does not have to relinquish full control over drones, as they still do interact within the airspace and ultimately fall under their jurisdiction, but they must be separated into their own category.

This would allow for regulations to be made specifically for drones, especially in regard to trespass and privacy.[293] States have

---

[288] *See Advisory on the Application of Federal Laws*, *supra* note 131.

[289] The location of the drone, location of the pilot, and federal preemption matters would all come into play in this situation.

[290] Planes are not capable of the type of reconnaissance or espionage that drones are. *See* Jason Snead & John-Michael Seibler, *Redefining "Aircraft," Defining "Drone": A Job for the 115th Congress*, HERITAGE FOUND. 2 (Jan. 13, 2017), https://www.heritage.org/sites/default/files/2017-01/LM-197_0.pdf [https://perma.cc/5WVL-RS49].

[291] *Id.*

[292] *See generally* Steve Calandrillo et al., *Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety*, 23 STAN. TECH. L. REV. 182 (2020).

[293] Most insurance policies have an "aircraft exclusion" in their terms; this would also allow damage by drones (arguably more common than damage by planes) to be covered by insurance claims. *See generally* Derrick J. Hahn, *General Aviation Aircraft Insurance: Provisions Denying Coverage for Breaches That Do Not Contribute to the Loss*, 64 J. AIR L. & COM. 675 (1999).

followed common law precedent when it comes to trespass issues and drones, meaning that they interpret the law as if the drone was an aircraft.[294] This would also allow for corporate espionage or cybercrime conducted by drones to fall under the appropriate area of the law rather than to be consumed by the FAA and FCC. Corporations and others[295] would then be allowed to defend themselves against drones, and they would only be at risk of facing civil liability rather than federal criminal charges.

III. RESPONSE TO COUNTER-ARGUMENTS

A. Mitigation of C-UAS Technology

Counter drone technology can be dangerous in the hands of a bad actor, but that, and the use of C-UAS in general, can easily be mitigated. The government could ensure that only valid corporations receive C-UAS technology through a licensing program and hold corporations to their reasonableness standard by creating a strict liability policy and set rules of engagement.

Corporations could go through a licensing and approval process before they are given access to purchase C-UAS technology.[296] Corporations must be able to show a specific, demonstrable need for such technology, and they should only be given technology that fits that specific need. For example, a corporation's headquarters where important meetings are held, but large amounts of data are not stored, may just require stronger drone detectors and radars rather than drone jammers or drone guns. In this scenario, a detector may alert the business to a threat, and then, they could take extra security precautions, both physical and cyber, to further secure their meeting. Additionally, if the regulations involving the FCC and drones were loosened, businesses in this instance, or perhaps in even more serious events

---

[294] *See, e.g.*, Boggs v. Merideth, No. 16-CV-00006, 2017 WL 1088093, at *2-3, *7-8 (W.D. Ky. Mar. 21, 2017). This means courts generally will not find that a drone is trespassing, even if it is flying over your backyard. *See generally* Brady Getlan, Recent Development, Boggs v. Merideth *and the Present and Future Laws and Regulations of Drone Usage*, 7 U. BALT. J. LAND & DEV. 1 (2017).

[295] Specifically, homeowners.

[296] C-UAS users could also be required to go through a testing procedure before receiving their license.

as well, could trigger the attacker drone's "return to base" function.[297] Companies that worry about their data centers falling under attack may be entitled to stronger security measures due to the amount and sensitivity of the data they are storing. Available options for them should include the entire spectrum of defenses, and it could be narrowed on a case-by-case basis.[298] Construction sites would be another circumstance that could be decided on a case-by-case basis in the licensing stage.

Corporations would also need to be held strictly liable for any damage done to drones or bystanders in the event of a false positive report of malfeasance. This would encourage corporations to be absolutely sure of an attack or hack before taking reasonable action and would lower the risk of corporations negatively interacting with all drones flying over their airspace. There must also be set rules of engagement created for corporations to follow before disruptive action is taken against an attacker drone.[299]

---

[297] *See* Joseph J. Vacek, *Counter-UAS Applications Illegal Under 18 U.S.C. § 32 Are Justified When Using a Reasonably Defensible Counter-UAS Strategy That Incorporates Risk and Compliance Categorizations*, 93 N.D. L. REV. 499, 505-07 (2018). As of this writing, this type of system would interrupt and intercept satellite communications, which is illegal under 18 U.S.C. Section 32 and the FCC's regulations. *Id.*; *Interception and Divulgence of Radio Communications*, FCC, https://www.fcc.gov/consumers/guides/interception-and-divulgence-radio-communications [https://perma.cc/NKC8-9JYY] (Jan. 13, 2021). This also might implicate the Aircraft Piracy/Sabotage Acts. *See Advisory on the Application of Federal Laws*, *supra* note 131.

[298] In this circumstance, data centers in heavily populated areas likely should not have access to drone jammers. This could lead to drones falling out of the sky and could pose significant risks to innocent bystanders. However, companies that house their data or are constructing sites in less populated areas should have the right to jammers as long as they assume the risk of civil liability. Companies that hold outsourced data should arguably be given the highest security measures.

[299] This can be formulated by looking at the activities of innocent drones versus bad actors. For example, hobbyist drone users are not allowed to fly at night. *See* 14 C.F.R. § 107.29. Therefore, it could be reasonably assumed that a drone flying at night may be operated by a bad actor. The recent passage of the proposed remote identification process by the FAA will be helpful. *See UAS Remote Identification Overview*, FAA, https://www.faa.gov/uas/getting_started/remote_id/ [https://perma.cc/52KX-VQUY] (Oct. 13, 2021, 12:06 PM). Remote identification is not enough on its own though—if someone is intelligent enough to carry out a complex espionage mission or cyberattack, they can likely spoof their location. *See also* Tung Yin, *Game of Drones: Defending Against Drone Terrorism*, 2 TEX. A&M L. REV. 635, 671 (2015) ("Assuming that we have the technological infrastructure in place to detect and neutralize small drones, identification presents less of a challenge because we do not have to be 100% accurate, so long as the mistakes are false positives (i.e., misidentifying an innocuous drone as a

B. Other Mitigation Techniques Are Not Adequate

There are currently procedures and systems in place that help to mitigate general mischievous drone activity, like geofencing and police intervention.[300] The FAA has also recently enacted a regulation that will require all drone pilots to equip their drones with the ability to be remotely identified.[301] These mitigation techniques, however, are inadequate to deal with the use of drones for corporate espionage and cyberattacks. They were created to handle situations of hobbyist drones not following the rules, not to handle situations of hackers and spies conducting espionage missions with drones. Additionally, a military program to protect corporations would not be helpful either.

Remote identification ("Remote ID") is "the ability of a drone in flight to provide identification and location information that can be received by other parties."[302] Though this is a good step in the right direction and will be useful in terms of establishing rules of engagement and determining friend versus foe, it could easily be bypassed by a bad actor or simply ignored.[303] Like Remote ID, geofencing could easily be bypassed.[304] There are several websites, found using a simple Google search, that provide instructions on how to bypass a geofence.[305]

Additionally, the FAA simply instructs police to report any bad actors in violation of their specific drone regulations.[306] Law

---

hostile one) rather than false negatives. This dynamic points in favor of an 'if in doubt, bring it down' strategy, at least in the airspace above high-value targets.") (footnote omitted).

[300] *See* Pritchard, *supra* note 36; *Understanding Your Authority: Handling Sightings and Reports*, FAA [hereinafter *Understanding Your Authority*], https://www.faa.gov/uas/public_safety_gov/sightings_reports/ [https://perma.cc/W4PD-BQR3] (Aug. 30, 2021, 10:35 AM).

[301] *See UAS Remote Identification Overview*, *supra* note 299.

[302] *Id.*

[303] DL Cade, *Everything Wrong with the FAA's Remote ID Proposal, and How to Help Change It*, PETAPIXEL (Feb. 27, 2020), https://petapixel.com/2020/02/27/everything-wrong-with-the-faas-remote-id-proposal-and-how-to-help-change-it/ [https://perma.cc/4QLQ-Q7E3].

[304] *See* Pritchard, *supra* note 36.

[305] *See, e.g.*, *DJI Spark*, NO LIMIT DRONEZ, https://nolimitdronez.com/spark?gclid=CjwKCAjwiaX8BRBZEiwAQQxGxwu5V44wU75ydLd4FC-BzKHbe7nCC4AVFp2I1KK0Ic9vwB8-pN4g7RoCLDEQAvD_BwE [https://perma.cc/HH44-9Z72] (last visited Jan. 8, 2022).

[306] *See Understanding Your Authority*, *supra* note 300.

enforcement does not have the authority or technology to proactively handle a drone attack.[307] As previously discussed, corporations do not have the time to wait for law enforcement to arrive at the scene and then to handle the drone threat. Allowing military actors to protect corporations presents a similar problem as the law enforcement protection scenario. Though the military does have authorization to use C-UAS technology,[308] this sort of approach would not be beneficial to corporations. Again, corporations must have their own protections in place to stop the espionage or hacking as it is happening—they do not have the time to wait for "backup" to handle the situation. This approach is also not economically sensible. There are not military posts in every city across the United States, nor should there be. Corporations should have access to self-help technology.

C. C-UAS Technology Is Used in a Successful Manner Elsewhere

Correctional facilities, military bases, and airports have access to commercial C-UAS technology.[309] Each has had some success in the monitoring and thwarting of drone activity in their airspace.[310] The successes of these systems utilized in each capacity support the argument that private business owners should have the right to such systems as well. The cost to society and the cost to the consumer of drone incidents are in no way greater at the aforementioned facilities than at a business headquarters or a data center—the costs are just different.

CONCLUSION

Today, corporate espionage has taken on a new and more dangerous form by using drones as the medium to conduct trade secret misappropriation and cyberattacks against unsuspecting businesses. Drones allow for physical attacks and cyberattacks to be carried out with ease. They are cheap, easily accessible, and easy to use. Drones can be used to conduct traditional, reconnaissance-

---

[307] *See id.*
[308] *See* Rupprecht, *supra* note 144.
[309] *See id.*
[310] *See id.*

type missions including spying, recording, and surveilling. However, they can also be used to hack systems, even those isolated from networks, cause data server outages, or spread malware. Drones can be utilized in the stealing of trade secrets and consumer information or even cause an interruption in the business's daily processes—each costing the corporation tremendously.

With this new use of drones in the realm of corporate espionage, corporations have few options when it comes to retaliation. The legal route is often unattractive as the damage has already been caused, the economic value is hard to assess, and it is difficult to litigate trade secret claims. This reactive choice of remedy is inadequate when compared to the potential proactive measures that corporations could take. C-UAS technology is mostly illegal in the United States, but corporations would greatly benefit if given authorization to utilize such systems.

The use of C-UAS technology is justified under self-help principles. The current laws in place do not provide equitable remedies, and C-UAS will not undermine law and order. There is little risk to society as corporations can be held strictly liable for any botched responses and the damage, likely minimal, they could potentially cause. Additionally, the reasonable-measures-of-protection standard established under trade secret law, and required by the FTC in protecting consumers' data, necessitates the use of C-UAS. The use of drones for the purpose of corporate espionage has also created an economic imbalance in the world of trade secret misappropriation, which the use of C-UAS could equilibrize.

Drones will become the future of corporate espionage, and corporations need to have the resources necessary to protect themselves from this current, and only growing, threat. The use of C-UAS technology is a proactive step, which is more beneficial to the company, than the traditional and ill-fitting reactive steps currently available. C-UAS technology is justifiable self-help necessary for the protection of trade secrets.