INSTITUTIONAL DOXING AND ATTRIBUTION: SEARCHING FOR SOLUTIONS TO A LAW-FREE ZONE

Kimberlee Styple[*]

TABLE OF CONTENTS

[*] J.D. Candidate, University of Georgia School of Law, 2022. B.A. in Criminology and Law, University of Florida, 2019. B.A. in English, University of Florida, 2019.

I. INTRODUCTION

You may not have heard of institutional doxing, but you should be afraid of it. Institutional doxing is a new concern arising from the invention of the Internet. The advent of the Internet in 1989 led to the development of a blinding array of new technology, none more striking than the World Wide Web.[1] According to the World Bank, in 2019 over fifty percent of the world's population had regular access to the Internet, amounting to billions of new cyberspace citizens.[2] While there are notable advantages of an increasingly digital society, increased digitalization has also made society more vulnerable.[3] Some of the most prevalent dangers are cyberattacks, specifically institutional doxing.

Many high-profile cases involving institutional doxing made international headlines in recent years.[4] These cases include the well-publicized hacks of Ashley Madison and Sony.[5] "[T]he most famous 'dumps,' such as those released by Edward Snowden, the Sony hackers, and the Ashley Madison hackers, have become household names."[6] The Sony Hack gained notoriety due to its public attribution to North Korea.[7] In the Sony Hack, the "North Korean government stole and published gigabytes of corporate email from Sony Pictures. This was part of a much larger doxing — a hack aimed at punishing the company for making a movie parodying the North Korean leader Kim Jong-un."[8]

Institutional doxing attacks are increasingly dangerous according to Director of National Intelligence James Clapper, who announced that cyberattacks surpassed terrorism as the number one threat facing the U.S. today.[9] Cyberattacks, such as doxing, impose "increasing costs to our businesses, to U.S. economic competitiveness and to national security."[10]

---

[1] *A Short History of the Web*, CERN, https://home.cern/science/computing/birth-web/short-history-web (last visited Sept. 9, 2021).
[2] INTERNATIONAL TELECOMMUNICATIONS UNION, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (last visited Sept. 9, 2021).
[3] Bruce Schneier, *The Meanest Email You Ever Wrote, Searchable on the Internet*, ATLANTIC (Sept. 8, 2015), https://www.theatlantic.com/technology/archive/2015/09/organizational-doxing-ashley-madison-hack/403900/.
[4] *Id.*
[5] *Id.*
[6] Colin J.A. Oldberg, *Organizational Doxing: Disaster on the Doorstep*, 15 COLO. TECH. L.J. 181, 183 (2016).
[7] Schneier, *supra* note 3.
[8] Schneier, *supra* note 3.
[9] Aaron Boyd, *DNI Clapper, Cyber bigger threat than terrorism*, FEDERAL TIMES (Feb. 4, 2016), https://www.federaltimes.com/management/2016/02/04/dni-clapper-cyber-bigger-threat-than-terrorism/.
[10] *Id.*

Consequently, "[a] legal framework for attribution would provide a critical stepping stone for enabling a regime to restrict and redress the harms of state-sponsored cyber-attacks" and make the Internet a safer place.[11]

However, there are two primary reasons why international law lacks a reliable attribution method for state-sponsored institutional doxing.[12] First, the nature of doxing renders treaties and agreements typically used for attribution ineffectual, and there are limited alternatives to identify, prosecute, and remedy cybercrimes.[13] Second, the lack of remedy is compounded by the general lack of consistent and effective attribution in international law.[14] Treaties, agreements, and best practices that have built the basis of international law attribution procedures are riddled with gaps.[15] These gaps can be ascribed to ambiguous attribution practices and inadequate international law relating to cybercrimes.[16]

To resolve institutional security concerns, the international community must address institutional doxing and the growing international threat to security. This Note will analyze how international law should address the threat and will proceed in four parts. Part One defines institutional doxing and summarizes its increasing dangers. Part Two introduces the international law of attribution. Part Three examines potential methods of attributing institutional doxing to guilty states and evaluates several treaties, agreements, and best practices within international and domestic law to determine if any satisfy international security needs. If no adequate solutions exist in international or domestic law, privatized attribution procedures will be scrutinized to determine if they can protect the interests of the institutions vulnerable to doxing. Part Four further evaluates the most promising solution and identify potential implementation issues. This Note concludes that the issue presented by institutional doxing and a lack of reliable attribution methods in international law would be best resolved by privatizing attribution procedures. Large multinational corporations, which are often the target of institutional doxing attacks, are often unprepared for both cyberattacks and attribution procedures that follow them.[17] In practice, these large multinational corporations have failed to efficiently attribute doxing

---

[11] Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376, 381 (2018), https://yjolt.org/sites/default/files/20_yale_j._l._tech._376.pdf.

[12] Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 524 (2020).

[13] *Id.*

[14] *Id.*

[15] John Billinger & Matthew Waxman, *Filling Gaps in International Law*, LAWFARE (Feb. 4, 2021, 10:21 AM), https://www.lawfareblog.com/filling-gaps-international-law.

[16] Eichensehr, *supra* note 12.

[17] Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR (Aug. 2, 2011), https://www.vanityfair.com/news/2011/09/chinese-hacking-201109.

perpetrators.[18] However, before this Note can properly analyze solutions, it must first contextualize institutional doxing and its underlying dangers.

II. BACKGROUND AND HISTORY

A. Introduction to Institutional Doxing

Doxing is a damaging and malicious form of cyberattack that is increasingly common as our world digitalizes.[19] Doxing is generally defined as the act of publishing private information, such as credit card numbers, addresses, phone numbers, medical information, or private communications.[20] Not all publishing of private information is doxing.[21] Notably, a key distinction between doxing and general cyberattacks is that the objective of doxing is mainly harassment, not whistleblowing. [22] This Note defines doxing as the act of weaponizing private information against an individual, institution, or state with an intent to harass or harm.

While doxing is becoming increasingly common, it is certainly not new.[23] Doxing is a subtype of online vigilantism that has existed since the origin of the Internet.[24] Doxing, "originally a slang term among hackers for obtaining and posting private documents about an individual, usually a rival or enemy" has existed on the Internet for decades.[25] However, doxing was originally a smaller-scale operation, consisting of "little black-hat hacker crews who were at war with each other — they would take docs, like documents, from a competing group and then claim they had 'dox' on them."[26] Over time, doxing attacks evolved into massive hacking operations that

---

[18] *Id.*
[19] Bruce Schneier, *2015: The year "doxing" will hit home*, BETA BOSTON (Dec. 31, 2014), http://www.betaboston.com/news/2014/12/31/2015-the-year-doxing-will-hit-home/.
[20] *Id.*
[21] *Id.*
[22] Bruce Schneir, *How to keep your private conversations private for real*, WASHINGTON POST (Mar. 10, 2017), https://www.washingtonpost.com/posteverything/wp/2017/03/08/conversations-online-are-forever-now-heres-how-to-keep-yours-private/.
[23] *Id.*
[24] Nellie Bowles, *How 'Doxxing' Became a Mainstream Tool in the Culture Wars,* THE NEW YORK TIMES (Aug. 30, 2017), https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html.
[25] *Id.*

[26] *Id.*

attacked corporations, law firms, individuals, and intelligence organizations like the NSA and the CIA.[27]

Institutional doxing is a subtype of doxing where hackers weaponize the Internet to collect and share a business organization's private information.[28] This includes information about customers, employees, board members, and trade secrets. Like standard doxing, the scale of an institutional doxing attack can vary. Institutional doxing can fluctuate from a disgruntled employee sharing a small business' private emails to large-scale professional hacks of multi-national corporations. Likewise, doxing technique can vary from "stealing data from an organization's network and indiscriminately dumping it all on the Internet" to precise data mining for a targeted attack on a specific department or project.[29] Although institutional doxing attacks may be conducted with vastly different methods and levels of severity, the devastating effects on collection and publication of proprietary, secret, or incriminating data with the intention to intimidate, harass, or humiliate a business organization remain the same.[30]

Corporations are increasingly attractive candidates for state-sponsored doxing attacks as they increase their size, influence, and economic force. Many institutional doxing attacks are committed by foreign states – one scholar notes that "state-sponsored cyber-attacks are on the rise and show no signs of abating."[31]

Some argue that corporations are acting as states in some capacities.[32] It could even be said that corporations act as the modern equivalent of traditional colonial powers by controlling large areas of resources and the livelihoods of many people. [33] Large multinational corporations, especially ones in the technology industry like Google, are "acting in some ways as nation-states used to act, exercising to the best of their ability some attributes traditionally associated with sovereign states."[34] In particular, "Facebook has become so powerful and omnipresent that some have begun to employ the language of nationhood to describe it."[35] Corporations' massive increase in power and influence made their intellectual property and trade secrets more valuable, making corporations more attractive doxing targets for foreign states.[36]

---

[27] *Id.*
[28] Oldberg, *supra* note 6.
[29] Schneier, *supra* note 3.
[30] *Id.*
[31] Tran, *supra* note 11, at 376.
[32] *See* Bruce Schneier, *The Rise of Political Doxing*, VICE (Oct.28, 2015, 8:00 AM), https://www.vice.com/en_us/article/z43bm8/the-rise-of-political-doxing.
[33] Gross, *supra* note 17.
[34] *Id.*
[35] Anupam Chander, *Facebookistan*, 90 N.C.L. REV. 1807, 1808 (2012).
[36] *See* Gross, *supra* note 17.

The relationship between business organizations and states is growing increasingly complex and will continue to evolve. This evolution will likely increase the amount and importance of interactions between states and corporations and increase the likelihood that they will clash on these issues. Therefore, as anti-corporate activism and targeted political sentiment grow, doxing is an increasingly popular and dangerous tool in the modern cyber-arsenal of states that should not be underestimated.[37]

The advent and continued practice of institutional doxing is a testament to the increased weaponization of information. Doxing's prevalence demonstrates that "information has value — particularly information related to people's identities, interests and habits."[38] "Doxing ultimately, makes data into a weapon."[39] As we enter "the age of big data," data is being recorded on an unprecedented scale.[40]

Many people share versions of themselves daily on Facebook, Instagram, and Twitter. Likewise, they have private conversations with others through Gmail accounts and Zoom calls. The companies people use to stay connected store accumulated personal data. It is "almost a given that you have personal information available online. Beyond social media and online discussion boards, there are public records of property ownership and voter registration, as well as massive databases of financial information assembled by credit-rating agencies."[41] The storage and maintenance of this personal data allows hackers to use doxing as a weapon. [42] One scholar who researched the risks associated with doxing attacks described that:

> [i]t often feels like everyone is collecting our personal information. Smartphone apps collect our location data. Google can draw a surprisingly intimate portrait of what we're thinking about from our Internet searches. Dating sites (even those less titillating than Ashley Madison), medical-information sites, and travel sites all have detailed portraits of who we are and where we go. Retailers save records of our purchases, and those databases are stored on the Internet. [43]

---

[37] *See* Schneier, *supra* note 32.
[38] Jasmine McNealy, *What is doxxing and why is it so scary?*, THE CONVERSATION (May 16, 2018, 6:26 AM), https://theconversation.com/what-is-doxxing-and-why-is-it-so-scary-95848.
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] Schneier, *supra* note 3.

The storage of this information also makes people vulnerable to doxing.[44] Those who are aware of the increasingly complete picture of our lives data can paint also understand its value and its potential as a weapon.[45] Those who intend to use data as a weapon understand that data brokers "have detailed dossiers that can include all of this and more."[46] The heightened value of data created an environment that encourages institutional doxing as a weapon and intensifies the harm that doxing can cause.

Corporations can suffer various types of harm from doxing attacks. Two types of potential harm corporations can suffer from doxing include embarrassment and negative press. For example, in the Sony Hack, the media primarily focused on "Sony's corporate executives, who had sniped at celebrities and made racist jokes about President Obama. But also buried in those emails were loves, losses, confidences, and private conversations of thousands of innocent employees."[47] Though "the press didn't bother with those emails—and we know nothing of any personal tragedies that resulted from their friends' searches" that information will forever remain accessible to the public.[48] Though the aim of the attack was primarily to hurt Sony, its employees "were caught in the blast radius of the larger attack" not aimed at them.[49]

In addition, victims of institutional doxing may suffer financial harm. For example, Sony's stock plummeted after the attack, hurting both Sony's finances and its investors.[50] Doxing attacks cause substantial financial loss, including costs for "the eventual investigation, consultants, lawsuits, stock price fluctuations, and more. The entire picture of a major compromise is the real value, as that is where companies can fully learn of the risks of a breach."[51]

Moreover, although corporations and their employees are the most immediate victims of institutional doxing, institutional doxing also harms customers. Since massive quantities of:

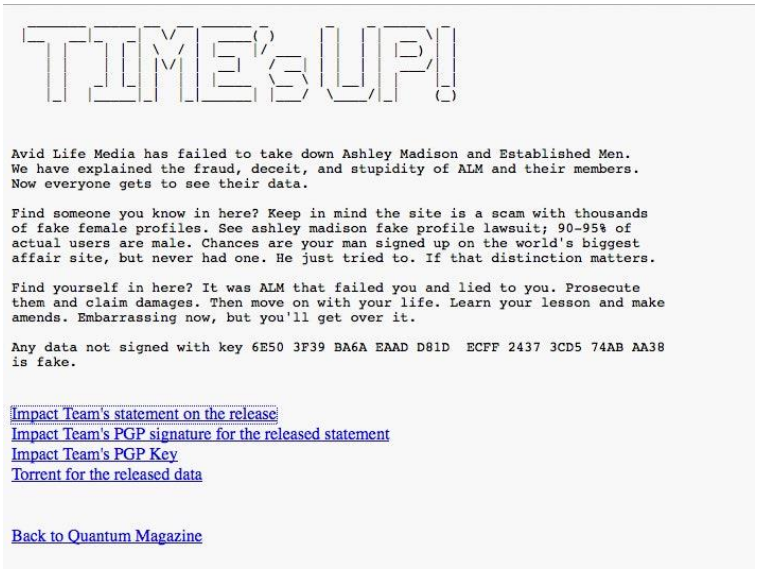
> our data is connected to the Internet, and stored in corporate networks, we are all in the potential blast-radius of these attacks. While the risk that any particular bit of data gets published is low, we have to start thinking about what could

---

[44] Oldberg, *supra* note 6.
[45] McNealy, *supra* note 38.
[46] Schneier, *supra* note 3.
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *A Breakdown and Analysis of the December, 2014 Sony Hack*, RISK BASED SECURITY (Dec. 5, 2014), https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.
[51] *Id.*

> happen if a larger-scale breach affects us or the people we care about. It's going to get a lot uglier before security improves.[52]

For those with sensitive information stored on corporate servers, the consequences of an institutional doxing attack can be life changing. The image below is the communication customers of Ashley Madison, a website for married men and women seeking affairs, received after hackers seized their information in an institutional doxing attack on Avid Life Media, the parent company of Ashley Madison.[53] When Avid Life Media did not take down Ashley Madison permanently in all forms the hackers released all customer records, including personal profiles with all the customers' secret sexual fantasies, matching credit card transactions, real names, home addresses, and employee documents and emails.[54]



Avid Life Media has failed to take down Ashley Madison and Established Men.
We have explained the fraud, deceit, and stupidity of ALM and their members.
Now everyone gets to see their data.

Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles. See ashley madison fake profile lawsuit; 90-95% of actual users are male. Chances are your man signed up on the world's biggest affair site, but never had one. He just tried to. If that distinction matters.

Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it.

Any data not signed with key 6E50 3F39 BA6A EAAD D81D ECFF 2437 3CD5 74AB AA38 is fake.

Impact Team's statement on the release
Impact Team's PGP signature for the released statement
Impact Team's PGP Key
Torrent for the released data

Back to Quantum Magazine

Although some users paid a fee for a "full delete" button, which, upon triggering, would remove any trace of their account, the attack showed that Ashley Madison was not actually fully anonymous and that the full delete button did not function as claimed. [55] Due to the doxing and release of

---

[52] Schneier, *supra* note 3.
[53] Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.
[54] *Id.*
[55] Oldberg, *supra* note 6, at 184.

sensitive personal information "people committed suicide, and countless lives were ruined."[56]

Furthermore, institutional doxing attacks may even harm those who had no relationship with the victimized corporation.[57] Examining the Ashely Madison Hack, doxers released false information along with the real user records.[58] As Ashley Madison's sign-up process did not require email verification to set up an account, some members of the site hijacked legitimate email addresses on the site.[59] For example, one of the hijacked email addresses in the data dump belonged to former UK Prime Minister, Tony Blair.[60]

Further, the risk of forged documents being included in doxing attacks is a growing concern. Russia recently began using forged documents in several disinformation campaigns—particularly relating to Sweden joining a military partnership with NATO and Russia's 2014 invasion of Ukraine.[61] While forging thousands of documents is difficult to accomplish, slipping a single forgery in a collection of real documents is more subtle.[62] One scholar theorizes that:

> Maybe a country that anonymously publishes another country's diplomatic cables wants to influence yet a third country, so adds some particularly egregious conversations about that third country. Or the next hacker who steals and publishes email from climate change researchers invents a bunch of over-the-top messages to make his political point even stronger. Or it could be personal: someone dumping email from thousands of users making changes in those by a friend, relative, or lover.[63]

As shown by the Ashley Madison, Sony, and Russian campaigns, the damage done by institutional doxing attacks can be widespread and severe. States that engage in or sponsor doxing attacks must be stopped. However, perpetrating states must first be identified and held accountable. Therefore,

---

[56] *Id.*
[57] Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] Bruce Schneier, *Organizational Doxing and Disinformation*, SCHNEIER ON SECURITY (Sept. 14, 2016, 6:21 AM), https://www.schneier.com/blog/archives/2016/09/organizational_1.html.
[62] *Id.*
[63] *Id.*

immediate action must be taken to find a reliable method of attribution for state-sponsored institutional doxing attacks.

B. Introduction to the Law of Attribution

How is it possible to stop an attacker when you do not even know their identity?[64] The inability to identify and attribute the source of doxing attacks allows bad actors to launch such attacks with impunity, "frustrating efforts at creating international laws or treaties to regulate this harmful behavior."[65] The concept of attribution involves allocating responsibility to a state for certain wrongful or illegal acts.[66] Generally, a party must attribute an act properly before international law can provide a remedy.[67] The importance of attribution "lies in the simple fact that states as legal persons can only act through natural persons. Without attribution the state is incapable of acting on the international plane."[68]

A variety of tribunals, state practices, and substantive norms helped shape international attribution.[69] For example, "[a]ttributing responsibility for cyberattacks to states . . . intersects with secondary international law rules regarding the evidence states must provide when accusing other states of internationally wrongful acts." [70]

There are two questions to ask in order to properly attribute a doxing attack to a state actor. The first question includes the act of attribution, to determine if the acts are an "(international) act of the State, one which is of relevance under international law." Then in the second question, one should ask if the act is "contrary to international law and therefore an 'internationally wrongful act of a State.'"[71] This two-step approach poses two sets of challenges. First, it may be difficult to determine which state was responsible for committing a specific act. Attribution could be complicated by the technology used in doxing attacks, and more traditional methods of avoiding responsibility.[72] Second, determining if the act was contrary to international

---

[64] Tran, *supra* note 11, at 6.
[65] *Id.*
[66] Kristen Boon, *Are Control Tests For the Future?*, 15 MELB. J. OF INT'L L. 1, 2 (2014).
[67] *Id.* at 45-46.
[68] Jörn Griebel & Milan Plücken, *New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia*, 21 LEIDEN J. OF INT'L L. 601, 602-603 (2008).
[69] *Id.* at 601.
[70] Eichensehr, *supra* note 12, at 523-24.
[71] Amina Alijacic, *Some Aspects of the Genocide Case and the (non)Achievement of Transitional Justice*, 1 INT'L J. RULE L., TRANSITIONAL JUST., AND HUM. RTS. 28 (2010).
[72] Eichensehr, *supra* note 12, at 528.

law involves additional inquiries relating to the underdeveloped body of international law.

Despite the existing framework, attribution is "an area of law that is notoriously underdeveloped even outside the cybersecurity context," leading to great difficulty in attributing doxing attacks.[73] Doxing attribution has technical, legal, and political issues involved in the process of assigning responsibility to the state or non-state actors responsible for an attack.[74] Moreover, states may go to great lengths to avoid detection for certain wrongful acts, making it even more difficult to attribute doxing.[75] Despite these challenges, a sufficient legal framework for attribution of doxing attacks is therefore a critical stepping stone to prevent and redress the harms of doxing.[76]

III. METHODS OF ATTRIBUTION

The search for an adequate solution is not without challenges. One scholar, when exploring this issue, wrote that "borrowing *lex generalis* from the non-cyberspace context is hard to do, and *lex specialis* governing evidence for cyberattack attribution has not yet crystallized."[77] In other words, general international law may be difficult or insufficient, and international law specific to attribution does not exist yet.[78] However, as addressed previously, institutional doxing attacks are increasingly dangerous. This makes finding a viable attribution method significant.

The motive behind this Note is to discuss potential solutions to some of the issues presented by institutional doxing. Therefore, this Note will not analyze all these issues in depth, but rather give a brief overview and discuss relevant applications.

The search for an effective attribution method for regulating state practices in cyberspace within existing international law has been unsuccessful thus far.[79] As discussed above, international law regarding attribution, and specifically cyberspace attribution, is limited.[80] This section will describe and discuss several existing international law tenants and whether they could be adapted to provide an attribution method for institutional doxing attacks.

---

[73] *Id.* at 524.
[74] *Id.* at 523.
[75] *See Id.*
[76] Tran, *supra* 11, at 5.
[77] Eichensehr, *supra* note 12, at 525.
[78] *Id.* at 524.
[79] *Id.*
[80] *Id.*

First, a solution will be sought in lex generalis. Lex generalis consists of all general international law regarding attribution.[81] Within the confines of this Note, articles of state responsibility, rule of war, and human rights treaties will be the primary focus. This Note will analyze and determine if there are any potentially viable solutions among them. Second, lex specialis, the limited international law directly applicable to cybercrime attribution, will be analyzed and a determination will be made if there are any potentially viable solutions.[82] The Tallin Manual 2.0 will be the sole focus of section two.[83]

Third, this Note will analyze proposed rules, treaties, or regulations applicable to cybercrime attribution and determine if there are any viable solutions. While section three will not be a comprehensive analysis of all proposals, it will focus on several of the most promising proposals.

Fourth, U.S. domestic law will be examined to see if there are viable domestic solutions that can meet the needs of the international community.

Lastly, private sector solutions will be analyzed, and a determination will be made if there are any potentially feasible solutions. A combined private and public sector approach will also be evaluated.

A. Lex Generalis

This section focuses on broad expressions of the international law of general applicability and will analyze it in the context of doxing attack attribution. This section covers the largest segment of international law. Although none of this law will be directly on-point to doxing attacks and cyber-attribution, it could supply a broad solution that could be tailored to doxing attacks and cyber-attribution proceedings.

i. ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts

"In 2001 after nearly four decades of work," the United Nations International Law Commission (ILC) adopted its Draft Articles on Responsibility of States for Internationally Wrongful Acts (Draft Articles). [84] The Draft Articles are a comprehensive set of rules relating to attribution procedures.[85] Since then, the United Nations General Assembly has

---

[81] Antoine Niedergang, *Lex Generalis and Lex Specialis*, SPACE LEGAL ISSUES (Nov. 24, 2019), https://www.spacelegalissues.com/lex-generalis-and-lex-specialis/.
[82] *Id.*
[83] *The Tallinn Manual*, CCDCOE, https://ccdcoe.org/research/tallinn-manual/ (last visited Oct. 1, 2021).
[84] Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?*, 95 TEX. L. REV. 1555, 1560 (2017).
[85] *Id.*

commended the Draft Articles to its member states. [86] It is possible that the Draft Articles have become customary international law, as few objections have been made.[87] Additionally, the Tallinn Manual 2.0 includes the Draft Articles and relies on them to define rules of state responsibility.[88]

Though there are different understandings of the "proposed altogether eight different attribution rules within Articles 4-11 of the ILC Articles," they all serve the same overall purpose, which is to calm the debate surrounding attribution in international law.[89] Specifically, the proposed rules of attribution reference whether individual conduct is attributable to the state.[90] The Draft Articles commentary describes the most authoritative guidance on the attribution parameters. The commentary to Article 5 of the Draft Articles "sets out three key conditions that must be satisfied in order for attribution to arise." [91] The first condition sets out that the conduct must equal an exercise of governmental authority.[92] The second condition sets out that the domestic law of the state must authorize the private actor to exercise this authority.[93] The third condition sets out that the actor must be exercising governmental authority at the pertinent time.[94] "These three factors alone determine the potential attribution of private conduct to the state pursuant to Article 5, but their practical meanings remain unclear."[95]

When applying the Draft Articles to institutional doxing, several issues immediately appear. While Draft Article 8 gives two examples where "the conduct of an individual or group of individuals may exceptionally be attributed to the State in two specific hypotheses," they are unreliable for attributing doxing attacks to the responsible states.[96] Draft Article 8 states that individual conduct can be attributed to a state:

> (a) if he, she or they were acting "in fact on behalf of the State"', i.e.-in the terms of Draft Article 8-if he, she or they were "in fact acting on the instructions of, or under the

---

[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] Griebel & Plücken, *supra* note 68, at 603.
[90] Santiago M. Villalpando, *Attribution of Conduct to the State: How the Rules of State Responsibility May Be Applied Within the WTO Dispute Settlement System***,** 5 J. INT'L ECON. L. 393, 396 (2002).
[91] Jennifer Maddocks, *Outsourcing of Governmental Functions in Contemporary Conflict: Rethinking the Issue of Attribution*, 59 VA. J. INT'L L. 47, 60 (2019).
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.* at 60-61.
[96] Villalpando, *supra* note 90, at 410.

> direction or control of, that State in carrying out the conduct'; or
>
> (b) "if and to the extent that the State acknowledges and adopts the conduct in question as its own." [97]

While Article 8 seemingly establishes reliable guidelines, it is more complex in practice. Regarding (a), it is already difficult for the victim to show that the individual cyber-criminal was state-sponsored and not a rogue actor, and technology makes this decision more difficult.

Furthermore, to establish state responsibility, the act must not only be harmful, "it must also amount to a breach of the offending State's international legal obligations." [98] Breaches of international legal obligations must be identified; this may be done either by act or omission.[99] "For responsibility to accrue to the State, the act must be attributable to the State, either as an act of 'its organs of government, or of others who have acted under the direction, instigation or control of those organs, i.e. as agents of the State.'"[100]

The Article 8 standard may provide clarity to standards of state responsibility. However, it is unclear whether the standard alone is sufficient to attribute cyber-crimes such as doxing to states. First, the Draft Articles have not given a clear answer to the international attribution problem because they do not specify the level of state control over an individual that is required for attribution.[101] Second, "to further complicate the issue of cyber accountability, states do not universally accept that the laws of state responsibility apply to cyber operations."[102] While most states recognize the laws as applicable in the cyber domain, the most recent meeting of the UN Group of Governmental Experts "fail[ed] to reach [a] consensus on the application of basic principles of international law in this context."[103] The Draft Articles alone, without amendment or further consensus, would fail to address institutional doxing.

---

[97] *Id.*
[98] Jensen & Watts, *supra* note 84.
[99] *Id.*
[100] *Id.*
[101] Elena Laura Álvarez Ortega, *La atribución de responsabilidad internacional a un estado por la conducta de particulares en el territorio de otro estado [The attribution of international responsibility to a State for conduct of private individuals within the territory of another State]*, 1 INDRET 34 (2015) (Spain).
[102] Maddocks, *supra* note 91, at 56.
[103] *Id.*

ii. Rule of War

The rule of war may apply to doxing attribution. The rule of war is:

> [t]he law that governs states and individuals in armed conflict. The law of war is both a part of international law that regulates the conduct of armed hostilities and a part of the law of the United States and of other nation-states that binds those individuals within its jurisdiction to comply.[104]

There are two issues to address to see if the rule of war applies to institutional doxing: (1) if doxing attacks are considered armed hostilities, and (2) if multinational corporations are state-like enough to participate in war per traditional international law standards.

Regarding the first issue, doxing attacks are increasingly popular in many state-versus-state conflicts.[105] In response to the rise of cyberattacks, states started recognizing cyberattacks as attacks.[106] For example, "[i]n May of 2011, the U.S. State Department released the Administration's International Strategy for Cyberspace, which indicated that the United States would consider certain cyber attacks as triggering its right to self-defense."[107] Likewise, "China announced the formation of an 'Online Blue Army' to complement its traditional Red Army."[108] Some scholars pose that doxing attacks on U.S. entities "now come within an analog of the Willie Sutton rule; that is, they are attacked because they are particularly attractive targets for . . . nation-states bent on war."[109]

However, one issue centers around that "[t]he law governing when states can resort to force, *jus ad bellum*, and the law governing states' conduct during armed conflict, *jus in bello*, were written with the kinetic realm in mind."[110] Besides the physical computers used to commit the purely digital hacks, doxing attacks barely relate with the kinetic realm.

Regarding the second issue, state action against a corporation may be characterized as an instigation of conflict that the rules of war could be applied to. Corporations and states share many characteristics, and multinational corporations act increasingly state-like. Some scholars use the term

---

[104] LAW OF WAR (LAW OF ARMED CONFLICT OR LOW OR LOAC), THE WOLTERS KLUWER BOUVIER LAW DICTIONARY DESK EDITION (2012).
[105] Susan W. Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 401-402 (2007).
[106] *Id.* at 386.
[107] Hannah Lobel, *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, 47 TEX. INT'L L.J. 617, 619 (2012).
[108] *Id.*
[109] Brenner, *supra* note 105, at 426-27.
[110] Lobel, *supra* note 107, at 626 (emphasis added).

"corporatocracy" to describe the state-like evolution of corporations, defined as "a tripartite financial and political power relationship between multinational corporations ('MNCs'), international banks, and governments."[111]

However, corporations, despite their expanding power and scope, are not recognized like states. In "other salient ways, the analogy runs out. Most obviously, the companies lack territory, statehood, and sovereignty--key features of countries. And countries by and large do not recognize the companies as fellow Westphalian entities."[112] It is widely accepted that "[t]he law of war is geared toward states" and this is unlikely to significantly change despite the real-world changes corporations have undergone.[113]

Lastly, attribution procedures in the rule of war may fail to meet the needs of institutional doxing, specifically the need to reliably attribute international doxing attacks. The law of war typically requires states attacking another state to identify themselves.[114] In traditional armed conflict:

> it is generally not difficult to identify the state responsible for an act of war in the real-world. The initial attack may be a surprise . . . but attributing the attack to a specific state tends to be a relatively simple process. Military attackers wear distinctive, uniform clothing and use equipment with insignias or characteristics indicating their national affiliation.[115]

However, identification in the cyber context is extremely technical and may prove to be more challenging than what traditional standards can meet. Therefore, it is unlikely that the rule of war provides an adequate attribution system for doxing attacks due to the covert and varied nature of cybercrime and the force-driven conceptualization of warfare. Despite its challenges, rule of war international law is one of the best attribution methods for larger-scale or repeated attacks. However, that is beyond the focus of this Note.

iii. Human Rights Treaties

Various human rights treaties may provide attribution procedures that could apply to doxing attack attribution. Human rights are a subject extensively covered by international law. "The international human rights

---

[111] Priti Nemani, *Globalization Versus Normative Policy: A Case Study on the Failure of the Barbie Doll in the Indian Market*, 13 ASIAN-PAC. L. & POL'Y J. 96, 99 (2011).
[112] Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 668 (2019).
[113] *See generally* Lobel, *supra* note 107, at 632.
[114] Brenner, *supra* note 105, at 406.
[115] *Id.*

regime has drawn on principles establishing rules of attribution of state responsibility such that individuals can now invoke those principles in front of human rights bodies," various tribunals, courts, treaties, and agreements developed to address human rights violations and to hold the perpetrators responsible.[116] Examples include the UN Human Rights Committee, the European Court of Human Rights, and the Inter-American Court and Commission of Human Rights. [117] These organizations have applied an expansive body of international law, and a possibly useful infrastructure for doxing attack and cyber-attribution proceedings.[118] Existing human rights infrastructure could apply to cyber-attribution proceedings, or even recognize cybersecurity as a human rights issue.[119]

Moreover, there is a growing trend of hearing cases regarding individuals claiming breaches of states' international human rights obligations.[120] Parallels could be made between the prosecution of war criminals sponsored by states and cybercriminals employed by states.

However, applying a human rights scheme in the cybercrime context is unlikely a viable long-term solution. "As criteria differ between general international law, [Organisation for Economic Co-operation and Development] standards, the law on state immunity, European human rights law, and Inter-American human rights law," it is difficult to determine what standards apply.[121] Moreover, UN member states are in conflict over whether cybersecurity is a human rights issue.[122] While Estonia, Belgium, the Netherlands, Ecuador, Japan, and Switzerland, among others, have recently advocated for an "'open, free and stable cyberspace where the rule of law fully applies, and human rights and fundamental freedoms are respected' . . . . Noticeably silent on rights were the two cyber heavyweights: the US, which didn't address the issue, and Russia, which didn't participate in the meeting."[123] When the two largest players refuse to even address the issue, it is unlikely that the human rights framework can provide reliable attribution procedures.

---

[116] Rachel A. Opie, *Human Rights Violations by Peacekeepers: Finding a Framework for Attribution of International Responsibility*, 2006 N.Z. L. REV. 1, 8 (2006).
[117] *Id.* at 8-9.
[118] *See generally id.*
[119] Deborah Brown, *It's Time to Treat Cybersecurity as a Human Rights Issue*, HUMAN RIGHTS WATCH (May 26, 2020, 6:02 PM), https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue.
[120] Opie, *supra* note 116, at 8-9.
[121] Judith Shönsteiner, *Attribution of State Responsibility for Actions or Omissions of State-Owned Enterprises in Human Rights Matters*, 40 U. PA. J. INT'L L. 895, 906 (2019).
[122] Brown, *supra* note 119.
[123] *Id.*

iv. Jurisprudence

International courts could provide a method of attribution suitable for institutional doxing. In particular, the jurisprudence of the European Court of Human Rights (ECtHR), the Inter-American Commission (IAC), the Inter-American Court of Human Rights (IACtHR) and the International Court of Justice (ICJ) could be looked to as significant indicators of attribution issues in international law.[124] Using international criminal courts to attribute acts is not new; courts previously provided state attribution.[125] The ICJ implements a distinct approach to international adjudication, providing a model for how international courts compel states to participate in their systems.[126]

For example, following the Iran-Contra Crisis, the United States was accused of aiding Contra forces in attempting to overthrow the Nicaraguan Government. To attribute the aid, Nicaragua brought the issue to trial via the ICJ.[127] In the case of *Nicaragua v. USA*, "the Court had to decide, among other issues, whether to uph[o]ld Nicaragua's claim that the United States had 'devised the strategy and directed the tactics of the contra force, and provided direct combat support for its military operations.'"[128] The issues raised in cases like *Nicaragua* can apply to doxing attribution. On a fundamental level, both involve finding and trying a state for perpetrating bad acts. Moreover, "[a]s a general matter, the ICJ has broad subject- matter jurisdiction to hear any international law claim brought before it, so long as it is brought with the consent of both parties."[129] The ICJ had not heard any disputes regarding cyberattacks but, these disputes are likely within its jurisdictional scope.[130]

These courts and their jurisprudence have set out several tests that could standardize a method of attribution for institutional doxing attacks. The ICJ applied two tests in *Nicaragua*.[131] Those two tests were the "strict control" test and the "effective control" test.[132] The "strict control" test is based on

---

[124] Shönsteiner, *supra* note 121, at 925.
[125] Shönsteiner, *supra* note 121.
[126] Tran, *supra* note 11, at 428; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, INTERNATIONAL COURT OF JUSTICE, https://www.icj-cij.org/en/case/70.
[127] Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

[128] Ortega, *supra* note 101, at 8.

[129] Tran, *supra* note 11, at 428.
[130] *Id.* at 431.

[131] Ortega, *supra* note 101, at 2.

[132] *Id.*

complete dependance, while "effective control" is based on partial dependance.[133] However, the ICJ held that the strict control test was not persuasive in the case of organized groups.[134]

In contrast, the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia ("ICTY") uses the "overall control" test.[135] The "overall control" test was created when "[t]he Appeals Chamber held that the conduct of the Bosnian Serb armed forces could be attributed to the Federal Republic of Yugoslavia, on the basis that these forces ′as a whole′ were under the overall control of that State."[136] The "overall control" test partially discards the ICJ′s ′effective control′s test.[137] Lastly, the European Court of Human Rights has developed the effective overall control test.[138]

Though all these tests are valuable, they likely fail to meet the needs of attributing international doxing. There is a distinct "tension between the need for what has been called 'real accountability' of States and the attribution of responsibility to States only for their own conduct."[139] A more significant issue is that there is no existing international body for attribution. While the existing framework would certainly work if applied to a court designated for attribution, there will likely be issues in creating that body.[140] This is troubling because it suggests that states are only incentivized to create these institutions when challenges result in disaster.[141] While this generalization is not final for practically implementing attribution law, it does make it less appealing in the search for a reliable and immediate attribution method.[142]

B. Lex Specialis

Next, this note will analyze narrow expressions of the international law of special applicability in the context of doxing attack attribution. In contrast to lex generalis, this section covers a more specific segment of international law. Some of lex specialis is directly on-point to doxing attacks

---

[133] Stefan Talmon, *The Responsibility of Outside Powers for Acts of Secessionist Entities*, 58 INT'L AND COMP. L. Q. 493, 498 (2009).
[134] *Id.* at 505.
[135] *Id.* at 504.
[136] *Id.* at 504-505.
[137] *Id.* at 508.

[138] Antonio Cassese, *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 THE EUR. J. OF INT'L L. 649, 667 (2007).

[139] Ortega, *supra* note 101, at 2.
[140] Tran, *supra* note 11, at 383.
[141] *Id.* at 431.
[142] *Id.*

and cyber-attribution and could apply to doxing attacks and cyber-attribution proceedings. However, lex specialis is limited in its size and applicability.

i. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations ("Tallinn Manual 2.0") is one of the few on-point pieces of international law regarding cybercrimes, including doxing attacks. It represents an attempt to regulate cyberoperations via international law.[143] Specifically, the Tallinn Manual 2.0:

> offers a comprehensive regulatory scheme (154 rules), laying out the general legal principles governing cyberoperations and their interaction with specialized international law regimes, such as human rights law, diplomatic law, space law, and telecommunication law. Most of the Tallinn Rules focus, however, on the interplay between cyberoperations and the use of force (addressing both *jus ad bellum* and *jus in bello*).[144]

For the Tallinn Manual 2.0 to successfully regulate cyber-attribution, certain expansions would have to be made. Chiefly, the Tallinn Manual would need to become binding law; it is currently not compulsory.[145]

ii. Domestic Law to Regulate Doxing Attack Attribution

If there are no suitable attribution methods in international law, domestic law could serve as an adequate replacement. While this section will focus on the United States, other states have their own statutory schemes that could be examined. In the U.S., attribution is governed by U.S. domestic legal standards.[146] This includes federal privacy legislation like the Graham Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act, Fair Credit Reporting Act, and the Cybersecurity Act of 2015.[147] In the U.S., formal attribution procedures match the federal indictment process, where "[f]ederal

---

[143] Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. OF INT'L L. 583 (2018).
[144] *Id.* at 584.
[145] Markus Reisner, *What the largest hacking attack in U.S. history could lead to*, ZENITH (Dec. 19, 2020), https://magazine.zenith.me/en/politics/attacks-fireeye-solarwind-orion.
[146] Eichensehr, *supra* note 12, at 572.
[147] Oldberg, *supra* note 6, at 193-94.

prosecutors present evidence to a grand jury, which 'may return an indictment if there is probable cause to believe that a crime has been committed by the persons indicted.'"[148] A grand jury only need be convinced that there is probable cause to indict a defendant for an alleged, which is a lower threshold than the beyond a reasonable doubt standard.[149] The Supreme Court explained that probable cause is not an exceptionally high bar; it only requires fair probability.[150] Therefore, the U.S. could attribute certain cyberattacks via grand jury or other similar bodies under the probable cause standard.

While this standard is reasonable, domestic attribution mechanisms are unlikely to serve as a viable solution for a variety of reasons. First, the variance is too great between nation states. While some nations implemented similar procedures, others are vastly different in protecting the accused.[151] Moreover, there is consensus that:

> reliance on varied domestic law standards to govern attributions is unlikely to generate consensus among states about how attributions should be made. For issues related to the permissibility (or not) of state behavior vis-à-vis other states, there is significant value in having *agreed* legal standards. States are coequal sovereigns in the international system, not usually subordinates governed by each other's domestic laws. Domestic legal standards--especially divergent ones--cannot reasonably be expected to generate cross-national agreement on the bounds of permissible state behavior any more than disparate policy choices can. That is the domain of international law.[152]

Therefore, it is highly unlikely that any state's domestic law would suitably replace the international law of cyberattack attribution.

IV. PROPOSED EXPANSIONS

This section discusses proposed expansions to international law regarding the law of attribution. As international law continues to evolve in response to new and updated problems, new proposals will be made, some of which may serve as adequate solutions to the issue at hand.

---

[148] Eichensehr, *supra* note 12, at 572; quoting Charles Alan Wright et al., *Federal Practice & Procedure Criminal* § 111 (4th ed. 2008).
[149] *Id.* at 572-73.
[150] *Id.* at 573.
[151] *Id.* at 575.
[152] *Id.* at 576.

A. Due Diligence

Two international law scholars proposed a potential solution to the attribution problem, derived from the international law concept of state responsibility for transboundary harm.[153] International law has increasingly held states responsible for their harmful activities.[154] One significant aspect of state responsibility is international accountability, as state responsibility often attaches for purposes of litigation, negotiations, or countermeasures.[155] Because of this significance, attribution of harmful acts may occur through a response proxy. A response proxy is "an entity against whom action is taken when action against a responsible party is not feasible." [156] By applying due diligence principles to cyberspace and their relationship to countermeasures "illustrates an initially attractive solution to the attribution dilemma."[157] The authors write that:

> Recognizing a cyber-specific obligation of due diligence to address emanation of such cyber harms might mitigate the attribution dilemma. That is, a primary rule of conduct requiring diligent management of territorial cyber infrastructure could give rise to responsibility on the part of non-diligent States as proxies for unidentified or unreachable malicious actors. Legal recognition of such breaches of diligence permits State victims of cyber harm to take action to induce compliance and terminate harm without necessarily tracing attribution to the original, difficult-to-identify source. Such an approach has gained momentum among both States and commentators.[158]

Although "due diligence could be an effective tool in justifying the use of countermeasures in the fight against the difficulties caused by the inability to attribute harmful cyber acts" it may also worsen the issue.[159] If applied too aggressively, proxy responses may act as counterproductive and create instability in the international system, as "[a]lthough development of primary rules of conduct in international law is generally thought to increase stability and cooperation, recognition and refinement of a duty of cyber due diligence might impose significant costs to security, stability, and even to international

---

[153] *See* Jensen & Watts, *supra* note 84.
[154] *Id.* at 1558.
[155] *Id.* at 1562-63.
[156] *Id.* at 1558.
[157] *Id.* at 1559.
[158] *Id.* at 1558.
[159] *Id.* at 1559.

law compliance."[160] Due to the likely instability in implementation, and the potential pushback from liable parties, a due diligence approach is not currently the preferred method of attributing doxing attacks.

B. Legalizing Cyberattack Attribution and Evidentiary Standards

Legalizing cyberattack attribution methods in conjunction with clear evidentiary standards for the attribution process may aid in developing a procedure to attribute institutional doxing attacks. Several nations including the U.S., United Kingdom, France, and the Netherlands hold that evidence-giving is not currently required for attribution within the scope of international law.[161] While some states practice providing evidence with their allegations, there is no legal standard that requires providing such evidence.[162] "Such 'trust us' attributions are problematic for any number of reasons."[163] Attributions without evidence may be incorrect, difficult to corroborate or debunk due to the lack of supporting evidence, or foster greater consolidation of blocs with respect to cybersecurity issues.[164] However, there are many potential positive effects of creating an evidentiary standard for cybercrime attribution as a method of improving institutional doxing attribution.[165]

While an attribution method is needed, and evidentiary standards are certainly a necessary component, it is difficult to implement these standards.[166] While there are many positive effects, the negative concerns outweigh these positive effects. There are distinct downsides to requiring evidence for doxing attack attribution. First, states may invoke the need to protect their confidential sources and methods.[167] While there are ways to attribute information without exposing confidential sources and methods, international evidentiary law would certainly heighten the risk. Second, "states may fear that a legal requirement to provide evidence would require more evidence than they currently provide as a matter of policy."[168] Third, verification problems may present themselves.[169] Fourth, progressive development of law relating to evidence to support attribution may have positive effects, support stability, and help avoid conflict over cyberspace.[170]

---

[160] *Id.* at 1558.
[161] Eichensehr, *supra* note 12, at 520.
[162] *Id.* at 526.
[163] *Id.* at 567.
[164] *Id.*
[165] *Id.* at 570-71.
[166] *Id.*
[167] *Id.* at 569.
[168] *Id.*
[169] *Id.* at 570.
[170] *Id.* at 570-71.

Moreover, setting a strict evidentiary standard may decrease the overall number of attributions.[171] This is undesirable considering the rising number of institutional doxing incidents that need attribution.

Further, non-state actors involved in the attribution-making process may refuse to share their sources and will not share those sources without a body of law to compel them to. Specifically, the victims of institutional doxing may make attributions, and international law would fail to regulate them easily as private parties. For example, when previously attributing a cyberattack to a state, Google refused to show how it acquired information or disclose any of its attribution methods. Likewise, Facebook stated that to protect the integrity of its methods and processes, it would not explain how it attributes attacks.[172] Regardless of evidentiary standards for attribution in international law, private parties reinforced that attribution is not just a state practice.[173]

In sum, while the benefit of establishing attribution procedures with a clear evidentiary standard may provide reliable and accurate results, the likelihood of persuading private parties to adopt evidentiary rules is unlikely. Therefore, establishing attribution procedures with clear evidentiary standards in international law is unlikely the best method going forward.

C. Joint effort: A New Public and Private Entity

Some discussion has revolved around creating a new international legal body to handle attribution questions. It was initially proposed by Microsoft in a 2016 White Paper.[174] There, Microsoft proposed to create an international institution for attributing state-sponsored cyberattacks led by a mix of governmental and nongovernmental actors. Modeled after the International Atomic Energy Agency, the proposed institution included technical experts from a variety of governments, the private sector, academia, and civil society.[175] Through the creation of such a body:

> Microsoft envisions that the organization would produce a "technical analysis of the attack and evidence of attribution," which it would sometimes publish. Microsoft acknowledges that the institution would need representatives from a 'diverse set of nation-states and geographic regions,'

---

[171] *Id.*
[172] Kristen Eichensehr, *Your Account May Have Been Targeted by State-Sponsored Actors: Attribution and Evidence of State-Sponsored Cyberattacks*, JUST SECURITY (Jan. 11, 2016), https://www.justsecurity.org/28731/your-account-targeted-state-sponsored-actors-attribution-evidence-state-sponsored-cyberattacks/.
[173] *Id.*
[174] Eichensehr, *supra* note 12, at 588.
[175] *Id.*

> including "[a]t a minimum . . . representatives from countries that are permanent members of the United Nations Security Council." The white paper further suggests that attribution reports 'can be subject to peer review, improving the quality of the results.'[176]

This model would also serve as an effective endorsement of private entities performing governmental functions in international law, potentially encouraging additional cooperation between the public and private sectors.[177]

Others proposed establishing a Global Cyber Attribution Consortium with "broad membership across geopolitical lines to foster a diversity of perspectives and to minimize the possibility that its findings are tainted by political influence."[178] Members of this organization could include experts in cybersecurity companies and academia, including legal, cyberspace, and international policy experts.[179] The University of Washington's School of Public Policy proposed a similar plan regarding an exclusively private sector international attribution organization.[180]

Microsoft's proposal takes a pragmatic approach. The problem of attribution may be solved most efficiently by a combination of international law and private sector action. Or more pessimistically, neither international law nor the private sector is capable of handling attribution of institutional doxing attacks on their own, and their cooperation is necessary. Combining existing international law institutions and forums with the capabilities of the private sector makes this proposal a viable solution.

However, there are implementation issues that render this option unusable. Chiefly, all the above-mentioned bodies are merely proposals. No concrete steps have been taken to make these institutions a reality. While the proposals may eventually be a viable solution, the international law community needs immediate action to attribute cybercrime, and the proposals are still limited to theory.

D. Private-Sector Attribution

It is unlikely that any of the public methods of attribution previously discussed would address institutional doxing. As outlined above, general

---

[176] *Id.* (*citing* SCOTT CHARNEY ET AL., MICROSOFT, FROM ARTICULATION TO IMPLEMENTATION: ENABLING PROGRESS ON CYBERSECURITY NORMS 11 (2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8 [https://perma.cc/E92D-BL9K]).
[177] Maddocks, *supra* note 91, at 80.
[178] Eichensehr, *supra* note 12, at 588-89 (quoting Intl'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001)).
[179] *Id.* at 589.
[180] *Id.*

international law attribution methods are unlikely to function adequately, and there are no effective existing specific attribution methods. Moreover, domestic law cannot suit the needs of attribution. The lack of viable legal solutions regarding attribution created a "law-free zone" surrounding effective cyber-attribution procedures.

The law free zone hinders institutional doxing victims from acquiring a proper remedy for being doxed. If international law cannot provide an adequate method of attribution, institutions should privatize the attribution process to ensure adequate procedure after such attacks. Where law has failed, the private sector should compensate.

The private sector is growing into the law-free zone. Some scholars have indicated that "[p]ublic attributions of state-sponsored cyberattacks have become one of the best sources of information the public has about state behavior in cyberspace."[181] There are many failures in the international law of attribution and individual states have at times been hesitant to attribute attacks because attribution could harm their relationships with other states. But corporations may lack this inhibition, especially when compensation incentivizes corporations to attribute doxers.[182]

For example, the Democratic National Committee (DNC) contracted the private company CrowdStrike following a July 2015 cyberattack.[183] CrowdStrike published the account of its DNC investigation, noting that its:

> Incident Response group was called by the Democratic National Committee (DNC), the formal governing body for the US Democratic Party, to respond to a suspected breach. We deployed our IR team and technology and immediately identified two sophisticated adversaries on the network – COZY BEAR and FANCY BEAR…. At DNC, COZY BEAR intrusion has been identified going back to summer of 2015, while FANCY BEAR separately breached the network in April 2016. . . [W]e had a high degree of confidence it was the Russian Government. And our analysts that looked at it and that had looked at these types of attacks before, many different types of attacks similar to this in different environments, certain tools that were used, certain methods by which they were moving in the environment, and looking at the types of data that was being

---

[181] Eichensehr, *supra* note 172.
[182] *Id.*
[183] *CrowdStrike's work with the Democratic National Committee: Setting the record straight*, CROWDSTRIKE (June 5, 2020), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

> targeted, that it was consistent with a nation-state adversary and associated with Russian intelligence.[184]

Later, the United States Senate issued a supportive report confirming CrowdStrike's attribution to Russia.[185]

Privatization also has the support of some involved in the U.S. government. In response to a cyberattack on Google's facilities, "Google openly asserted its view that the attack originated in China," and after being briefed by Google on the allegations, then Secretary of State Hillary Clinton, issued a statement that said, "[w]e look to the Chinese government for an explanation."[186] In response to another cyberattack, a former Assistant Attorney General for the National Security Division testified that "[a] lot of — outside of any political organization, companies, most corporations, they often would use these third party contractors, who they hired through their own counsel, and maximize the control from the point of view of the victim."[187]

The number of former governmental service companies that are providing private attribution services are rising and will likely continue to grow.[188] All sectors of government, from railways and prisons to military-related activities in combat zones, have increased privatization and outsourcing.[189] The trend is equally evident in cyberspace, where private actors play a role in upholding cybersecurity and engage in operations on states' behalf.[190]

In fact, corporations started to self-regulate their cyber-activities,[191] which suggests they may be able to further regulate attribution procedures. Specifically, as the culmination of an effort by Microsoft President Brad Smith, more than sixty tech companies from the United States and Europe signed a Cybersecurity Tech Accord ("the Accord").[192] "The Accord commits the companies to 'strive to protect all of [their] users and customers from cyberattacks . . . irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.'"[193] The Accord's signatories also vowed that they would not help governments conduct cyberattacks against any innocent citizens or enterprises.[194] The

---

[184] *Id.*
[185] *Id.*
[186] Gross, *supra* note 17.
[187] Crowdstrike, *supra* note 183.
[188] Jennifer Maddocks, *supra* note 91.
[189] *Id.*
[190] *Id.*
[191] Eichensehr, *supra* note 112.
[192] *Id.*
[193] *Id.*
[194] *Id.*

Accord's signatories include leaders in the technology industry, such as Cisco, Microsoft, Facebook, FireEye, Symantec, Nokia, and Telefónica.[195]

However, one potential risk of privatization is the increasing influence of corporations on international law. If states routinely dox corporations, and states respond with private-sector remedies, a method of punishment for the bad actor in international law still needs to exist. Without punishing guilty states, the situation could devolve going forward, with mega-corporations and states getting involved in conflict, or even all-out war. Corporations may make wrongful or incorrect attributions, and without evidentiary standards mandated by international law, they may go unremedied. Further, though corporations may not share the same political motivations, they do have some conflicting motivations, including profit. Google's post on the notifications explains: "[y]ou might ask how we know this activity is state-sponsored. We can't go into the details without giving away information that would be helpful to these bad actors, but our detailed analysis- as well as victim reports- strongly suggest the involvement of states or groups that are state-sponsored."[196] Similarly, Facebook explained that "To protect the integrity of our methods and processes, we often won't be able to explain how we attribute certain attacks to suspected attackers."[197] While Facebook and Google's statements mirror traditional statements by states in their own attribution procedures,[198] these changes are still concerning going forward.

However, privatizing attribution is still the best option until international law can adopt to the twenty-first century and create binding law on cyberattack attribution, against both states and private entities.

Privatizing attribution, at least in the context of institutional doxing is likely the most realistic solution. Corporations can outsource attribution quickly and effectively to private companies and then seek remedial measures. Those private companies will control the process and the substantive information. Additionally, multiple attributers in both the private and public sector increases the success rate of public attributions and achieve the desired goals of attributions.[199]

V. CONCLUSION

It is likely that doxing attacks will become more common and more severe as new technology develops and even more valuable data is stored online. Reliable attribution methods, whether within international law or in

---

[195] *Id.*
[196] Eichensehr, *supra* note 172.
[197] *Id.*
[198] *Id.*
[199] *Id.*

the private sector, are necessary for the safety of an increasingly data-driven world.

Privatized attribution procedures have successfully been applied and could conceivably be applied on a larger scale to match the threat of future doxing attacks. While past success is not the sole indicator of future value, it certainly provides an advantage over theoretical methods of attribution in international law. Further, privatizing attribution procedures encourage victim self-help. This could lead to taking additional cybersecurity precautions to avoid the cost of attribution, which would lower the overall harm of institutional doxing attacks.

However, it is important to consider that attribution only comes into play after the damage has already been done. While reliable attribution procedures are certainly needed to punish offenders and deter potential cybercriminals, this does little to remedy the harm done to the organization which had their private information posted publicly, in perpetuity. It is likely that "[f]orever secrets, like the formula for Coca-Cola, are few and far between. The one exception is embarrassments. If an organization had to assume that anything it did would become public in a few years, people within that organization would behave differently."[200]

While reliable methods of attribution are necessary to deter doxing attacks, corporations should carefully consider what information they collect and store. It is unlikely that the stored information will remain private for long. Cybersecurity is recognizing increasingly sophisticated threats and preventive measures are not always effective. Technology is now fundamentally intertwined with policy.[201] All levels of our society are building complex socio-technical systems and "[s]oftware constrains behaviour with an efficiency that no law can match."[202] Technology and policy are changing so rapidly that getting it wrong can be catastrophic.[203] Even if the best attribution procedures in the world are established, accepted, and utilized; and the culprit is caught, tried, and punished, the Internet never forgets.

---

[200] Schneier, *supra* note 61.

[201] Bruce Schneier, *We Must Bridge the Gap Between Technology and Policymaking. Our Future Depends on it*, WORLD ECON. FORUM (Nov. 12, 2019), https://www.schneier.com/essays/archives/2019/11/we_must_bridge_the_g.html.

[202] *Id.*

[203] *Id.*