IS IT TIME FOR A NATIONAL CYBERSECURITY SAFETY BOARD?

EXAMINING THE POLICY IMPLICATIONS AND POLITICAL PUSHBACK

*Scott J. Shackelford J.D., Ph.D.**

*Austin E. Brady***

ABSTRACT

In the wake of a series of destabilizing and damaging cyber attacks ranging from Equifax to Yahoo!, there has been a growing call for the U.S. government to establish an analogue of the National Transportation Safety Board (NTSB) to investigate cyber attacks. Even the esteemed Center for Strategic and International Studies has advocated for this approach in its policy recommendations to the 45th President. But how would such a Board function, and could it succeed where past public-private collaborations have failed given the rapid pace of technical innovation in the cybersecurity field? This Article investigates this policy prescription by researching the passage of the original NTSB, assessing the various proposals that have been made to establish a National Cybersecurity Safety Board (NCSB), and globalizing the discussion to ascertain how other nations are approaching this same issue.

INTRODUCTION

Back in 1926, a new technology was causing people to interact with the world in new ways, closing distances and linking together far-flung places, but in the process, also leading to a spate of personal injuries and deaths.[1] That technology was the burgeoning aircraft industry. In response, Congress passed the Air Commerce Act of 1926 to investigate aircraft accidents,[2] a step which, nearly 40 years later, gave birth to the Department of Transportation (DoT) in 1967.[3] The DoT included the National Transportation Safety Board, an independent agency charged with investigating the safety of various transportation systems, from highways and pipelines to railroads and airplanes.[4] Since then, the NTSB has investigated more than 130,000 accidents.[5] Now, nearly a century after the original Air Commerce Act, it might be time to learn from this legacy as we seek to understand how best to mitigate the risk of a threat to another new technology that is tying the world closer together even as it threatens our shared security—cyber attacks.

In the wake of a series of destabilizing and damaging cyber

* Chair, Indiana University-Bloomington Cybersecurity Program; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Associate Professor, Indiana University Kelley School of Business.
** J.D. candidate, Indiana University Maurer School of Law; M.S. Cybersecurity Risk Management candidate, Indiana University-Bloomington Cybersecurity Program.

[1] *See, e.g.*, Ben Rothke, *It's Time for a National Cybersecurity Safety Board*, CSO (Feb. 19, 2015), https://www.csoonline.com/article/2886326/security-awareness/it-s-time-for-a-national-cybersecurity-safety-board-ncsb.html (discussing national disasters). *See also History of The National Transportation Safety Board*, NAT'L TRANSP. SAFETY BOARD, https://www.ntsb.gov/about/history/Pages/default.aspx (discussing the history of the NTSB) [hereinafter, *NTSB History*].

[2] Air Commerce Act, Pub. L. No. 69-254, 44 Stat. 568 (1926).

[3] *NTSB History*, *supra* note 1.

[4] *Id.*

[5] *Id.*

attacks, there has been a growing chorus of calls to establish an analogue of the NTSB to investigate cyber attacks.[6] Far from being a niche proposition, the Center for Strategic and International Studies put its substantial weight behind this approach in its policy recommendations to the 45th President.[7] But how would such a Board function? And could it succeed where past public-private collaborations have failed given the rapid pace of technical innovation in the cybersecurity field?[8] This Article investigates this policy prescription by researching the passage of the original NTSB, assessing the various proposals to establish a National Cybersecurity Safety Board (NCSB), and globalizing the discussion to ascertain how other nations are approaching this same issue.

This Article is structured as follows: Part I examines the historical evolution and political calculus of the NTSB to provide a framework for discussion. Part II analyzes the various proposals for a NCSB, including both the policy implications and perspectives from leading public and private-sector stakeholders. Finally, Part III offers global insights about how other jurisdictions have similarly examined this concept, focusing on the European Union's pending General Data Privacy Regulation (GDPR) and Network Information Security (NIS) Directive.

I. NTSB ORIGINS

True to the spirit of the pre-*Lochner* era, regulation of the skies came slowly and haltingly, often requiring public calamities to spur legislative action. In the years following the First World War, pilots were subject to scant laws during what Federal Aviation Administration historian Nick A. Komons calls the "Chaos of Laissez Faire in the Air"[9] that resonates with modern concerns over a tragedy of the cyber pseudo commons.[10] The federal

---

[6] *See, e.g.*, NAT'L SCI. FOUND., INTERDISCIPLINARY PATHWAYS TOWARDS A MORE SECURE INTERNET 21 (2014) [hereinafter INTERDISCIPLINARY PATHWAYS].

[7] CTR. FOR STRATEGIC & INT'L STUD., FROM AWARENESS TO ACTION: A CYBERSECURITY AGENDA FOR THE 45TH PRESIDENT (2017).

[8] *See generally* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467 (2017) (for a discussion of the current state of public-private cybersecurity partnerships).

[9] NICK A. KOMONS, BONFIRES TO BEACONS: FEDERAL CIVIL AVIATION POLICY UNDER THE AIR COMMERCE ACT 1926–1938 7 (1978) [hereinafter KOMONS].

[10] *See* Michael Chertoff, *Foreword to JNSLP Cybersecurity Symposium*, 4 J. NAT'L SEC. L. & POL'Y 1, 2 (2010) ("Our reliance on cyberspace without adequate cybersecurity presents a potential tragedy of the commons scenario unfolding

government's wait-and-see approach stifled investment in air travel,[11] leading to a confusing patchwork of state and local laws.[12] Regulation of the skies was a hard sell for a tight-fisted Congress. Persuaded by a combination of abysmal safety statistics, and cries for regulation from the aviation industry itself,[13] Congress enacted the Air Commerce Act of 1926.[14] It gave federal oversight of aviation to the Department of Commerce's (DOC) new Aeronautics Branch, recognizing the potential air travel had for economic growth.[15] Federal attention revived the floundering industry, and aviation use took off over the next decade.[16]

The Air Commerce Act provided the legislative "cornerstone"[17] for increasing aerial safety. But it was not a perfect solution. *Lochner*-era federalism restrictions meant that only pilots and aircraft engaged in interstate commerce were subject to DOC regulations, such as licensing requirements and safety standards. Intrastate regulation was, predictably, left to the states.[18] Intra or inter, whenever accidents occurred, responsibility for investigating and assigning probable cause was vested in the Bureau of Air Commerce.[19] This role put the Bureau in the spotlight during investigations into the deaths of national figures—such as the 1931 demise of Notre Dame football coach Knute Rockne—making it subject to harsh scrutiny during the ensuing public furor.[20]

---

before us.").

[11] *See* KOMONS, *supra* note 9, at 29 (explaining that investors, insurers, and passengers were all reticent toward participating in the aviation industry).

[12] *Id.* at 27.

[13] The aviation industry averaged 70.8 deaths per year from 1921–1925. *Id.* at 23. While this number may seem low, consider that there were 347 total general aviation deaths in fiscal year 2017. *Fact Sheet—General Aviation Safety*, FED. AVIATION ADMIN. (Oct. 24, 2017), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=21274.

[14] Air Commerce Act of 1926.

[15] *See* AERONAUTICAL CHAMBER OF COM. OF AM., AIRCRAFT YEAR BOOK 7 (1927) (describing the unintentional development of a special Aerona utics Division in the Bureau of Standards).

[16] *See Small Open Cockpit Airplanes Lead in Aircraft Production*, 7(1) AIR COM. BULL. 4, 7 (1935) ("Of 8,733 airplanes in service on June 1, 1935, 2,414 were built in 1929").

[17] *See* KOMONS, *supra* note 9, at 88 (stating "[t]he Air Commerce Act will be the agency through which air transport will come into its own.").

[18] *Need for Uniform State Legislation*, 1(1) AIR COM. BULL. 1, 1–2 (1929).

[19] KOMONS, *supra* note 9, at 277.

[20] *Id*. at 278. *See also* Robert F. Kelley, *Knute Rock[n]e Dies with Seven Others in Mail Plane Dive*, THE NEW YORK TIMES (Apr. 1, 1931), https://archive.nytimes.com/www.nytimes.com/learning/general/onthisday/bday/0304.html (for

As it struggled with its national image, the Bureau had a separate, structural problem. Namely, the conflict-laden reality of the Bureau investigating the effectiveness of its own safety policies while it alone determined legally-binding fault.[21] It was not until the Civil Aeronautics Act (CAA) of 1938 that probable cause determinations were separated from the safety regulating functions and placed within a separate Air Safety Board.[22]

In forming the Air Safety Board, Congress affirmed the need for a dedicated corps of federal investigators to examine the causes of transportation incidents.[23] The growing pains over two decades, the deaths of a United States Senator and beloved Notre Dame football coach, and multiple bureau reorganizations solidified the need to split regulatory functions from investigations assigning fault. The formation of the Air Safety Board was a critical first step toward independent investigations; however, when Congress created the Department of Transportation (DOT) in 1967, it established the NTSB as an "independent" agency within the DOT.[24] This move created a different conflict of interest at a departmental level that was tasked with regulatory responsibilities at odds with the NTSB objective analysis. Finally, the NTSB was cleaved from DOT pressures in 1974, with Congress remarking that "[n]o federal agency can properly perform such (investigatory) functions unless it is totally separate and independent from any other . . . agency of the United States."[25] Once it was free of DOT administration, the NTSB came into its

---

Rockne's obituary); KOMONS, *supra* note 9, at 359–60, 370. Some suggested the plane crash that left Sen. Bronson Cutting dead may spell the end for the Bureau of Air Commerce. The Bureau spent 1936—after the Cutting crash—assuming control of air traffic control but could not demand air carriers follow their safety regulations like the Interstate Commerce Commission could with railroads.

[21] *See* KOMONS, *supra* note 9, at 278 (explaining further that part of the problem with the Bureau assuming responsibility for determining probable cause was that they might find that responsibility lay at the feet of the Bureau itself. This liability caused the Board's investigations to be less transparent, an unacceptable veil to an American public that demanded answers after high-profile deaths such as Sen. Cutting of New Mexico in 1935. A 1934 amendment to the Air Commerce Act had partially alleviated the secrecy problems but did not address the independence issue. The amendment mandated public disclosure of Bureau findings and forbade the findings of the Bureau from being admitted as evidence in legal proceedings.).

[22] *Id.* at 379.

[23] *See NTSB History*, *supra* note 1 (stating Congress' intent in creating the NTSB was to give a single organization the task of investigating all transportation accidents).

[24] *Id.*

[25] *Id.*

own as a fully independent investigatory agency.[26]

Concerns of overreaching federalism stunted growth in the beginning,[27] but the lesson of the NTSB is that a specialized organization can in fact promote the growth of highly-complex industries while boosting security for the public. However, that organization must be able to independently conduct its investigations without the fear of intra-agency meddling. Today, air travel is widely regarded as among the safest forms of mass transportation.[28] Can the same feat be replicated in cyberspace?

II. EXAMINING PROPOSALS FOR A NATIONAL CYBERSECURITY SAFETY BOARD

Propositions for strengthening U.S. cybersecurity range widely, from the creation of a repository of cyber incident data such as has been suggested through DHS to allowing companies to have a freer hand to engage in proactive cybersecurity measures.[29] A common refrain across many of these proposals, though, are more robust data breach investigation requirements, which could include "on-site gathering of data on why the attack succeeded, [so as] to help other companies prevent similar attacks."[30] This evokes one of the core functions of the NTSB, that is, to investigate and establish the facts behind an incident, and to make recommendations to help ensure that similar events do not occur in the future.[31] In short, investigators help establish "the who, what, where, when,

---

[26] *Id.*

[27] See KOMONS, supra note 9, at 85–88 (discussing the Board's history and early challenges).

[28] *See Transportation Fatalities by Mode*, DEP'T OF TRANSP., https://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_02_01.html (for a comparison of fatalities by method of transportation).

[29] *See, e.g.*, Amanda N. Craig et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52(4) AM. BUS. LAW J. 721, 722 (2015); Joe Uchill, *New Bill Would Allow Hacking Victims to 'Hack Back*,' THE HILL (Oct. 13, 2017), http://thehill.com/policy/cybersecurity/355305-hack-back-bill-hits-house. The DHS's Cyber Incident Data and Analysis Repository (CIDAR) would, if implemented, fulfill some of the core functions of an NCSB by enabling stakeholders "to anonymously share, store, aggregate, and analyze sensitive cyber incident data." *Enhancing Resilience through Cyber Incident Data Sharing and Analysis*, DEP'T HOMELAND SEC. 2 (2015), https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf.

[30] Robert K. Knake, *Creating a Federally Sponsored Cyber Insurance Program*, COUNCIL ON FOREIGN RELATIONS (Nov. 22, 2016), https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program.

[31] *Id.*

how and [perhaps] why behind an incident."[32] After the facts are determined, policymakers can, and often have, backed up NTSB recommendations with new regulations.[33] Failing that, it is common for air carriers, for example, to voluntarily implement such recommendations, such as through industry codes of conduct.[34]

The framework of an NTSB investigation—root cause determination of an accident and the development of proposals to avoid such failures in the future—is appropriate for high-complexity sectors beyond aviation. A useful comparison can be made to similar inquiries into NASA's space travel efforts. After the tragic explosion of the space shuttle *Columbia*, NASA put together an investigation board in order to determine what had caused the Shuttle to break apart upon reentry.[35] While proximate cause of the *Columbia* disaster was traced to a piece of insulating foam that dislodged and impacted the Shuttle's wing during liftoff,[36] the Columbia Accident Investigation Board (CAIB) assigned actual, or but for, cause to the overall culture at NASA.[37] The CAIB, similar to a thorough NTSB investigation,[38] expanded their investigation beyond the technical failures that led to the accident and into cultural causes. They laid part of the blame on the mosaic of events that created a culture of savings over safety at NASA during the post-Apollo period.[39]

Today, the business of space travel is still highly dangerous[40]

---

[32] INTERDISCIPLINARY PATHWAYS, *supra* note 6, at 21.

[33] Scott J. Shackelford, *What Cybersecurity Investigators Can Learn from Airplane Crashes,* THE CONVERSATION (Feb. 21, 2018), https://theconversation.com/what-cybersecurity-investigators-can-learn-from-airplane-crashes-91177.

[34] *See, e.g.*, *AdvaMed Medical Device Cybersecurity Foundational Principles*, ADVAMED, https://www.advamed.org/sites/default/files/resource/advamed_medical_device_cybersecurity_principles_final.pdf (highlighting, as an example, AdvaMed's efforts to enhance the security of medical devices).

[35] COLUMBIA ACCIDENT INVESTIGATION BOARD REPORT VOLUME I 6 (2003) [hereinafter CAIB].

[36] *Id.* at 49 ("The physical cause of the loss of *Columbia* and its crew was a breach in the Thermal Protection System . . . initiated by a piece of insulating foam.").

[37] *Id.* at 97 ("In our view, the NASA organizational culture has as much to do with this accident as the foam.").

[38] *See, e.g.*, NAT'L TRANSP. SAFETY BD., ACCIDENT REPORT NTSB/HAR-12/01 viii (2012) ("This accident is one of many investigated by the NTSB in which the motor carrier's safety processes, as well as its corporate culture, may have set the stage for the [accident].").

[39] CAIB, *supra* note 35, at 103.

[40] *See, e.g.*, Eric Berger, *The Second Launch from Russia's New Spaceport Has*

and costly.[41] However, relatively few people "slip[] the surly bonds of Earth"[42] and travel higher in the atmosphere than those at the cruising altitude of the major airlines. In fact, as of this writing, only six people reside in orbital space aboard the International Space Station.[43] Still, highly technical accidents require a qualified investigative body to comb through facts and determine causes, which, at times, include detrimental organizational norms.[44] Commercial actors in space travel, such as SpaceX and Virgin Galactic, still rely on the NTSB for post-accident investigations.[45] If space travel becomes more ubiquitous, we may see similar culture failures to those replete in the cybersecurity context.[46]

The CAIB's authority to expand its investigation beyond technical considerations and into cultural issues is a critical tool that a NCSB should also adopt. Like aviation, enhancing security in the emerging Internet of Everything is a highly complex, technologically and legally challenging endeavor where organizational culture can vary dramatically.[47] As companies, individuals, and devices continue to be integrated, the need for a NCSB may become as essential as the NTSB or CAIB. As the CAIB

Failed, ARS TECHNICA (Nov. 28, 2017), https://arstechnica.com/science/2017/11/the-second-launch-from-russias-new-spaceport-has-failed/; Alan Yuhas, *SpaceX's Booms and Busts: Spaceflight Is Littered with Explosions and Disasters*, THE GUARDIAN (Sept. 1, 2016), https://www.theguardian.com/science/2016/sep/01/spacex-falcon-9-explosion-tesla-elon-musk-nasa.

[41] *See* CAIB, *supra* note 35, at 103–09 (for further discussion of costs and budget constraints).

[42] JOHN GILLESPIE MAGEE, JR., HIGH FLIGHT (1941).

[43] *What is the International Space Station?*, NASA (Feb. 7, 2018), https://www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-the-iss-58.html.

[44] *See* CAIB, *supra* note 35, at 99 (mentioning that independent boards were commissioned following both the *Challenger* and *Columbia* accidents).

[45] Loren Grush, *SpaceX Eyes January 8th Return to Flight After Finishing Up Accident Investigation*, THE VERGE (Jan. 2, 2017), https://www.theverge.com/2017/1/2/14142064/spacex-flight-launch-date-falcon-9-explosion-investigation; NAT'L TRANSP. SAFETY BD., AEROSPACE ACCIDENT REPORT NTSB/AAR-15/02 (2015).

[46] *See, e.g.*, Andrew G. Simpson, *5 Reasons Cyber Security Is Failing and What P/C Insurers Can Do About It*, INSURANCE JOURNAL (Aug. 18, 2017), https://www.insurancejournal.com/news/national/2017/08/18/461482.htm (addressing five reasons cybersecurity has been ineffective, including the culture within organizations).

[47] *See* Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J. L. & TECH. 167, 171 (2008) ("There is a culture of pushing attackers away from oneself without any consideration of the poor overall security resulting from this lack of coordination between organizations.").

concluded:

> Attempting to manage high-risk technologies while minimizing failures is an extraordinary challenge. By their nature, these complex technologies are intricate, with many interrelated parts. Standing alone, the components may be well understood and have failure modes that can be anticipated. Yet when these components are integrated into a larger system, unanticipated interactions can occur that lead to catastrophic outcomes. The risk of these complex systems is increased when they are produced and operated by complex organizations that also break down in unanticipated ways.[48]

Like a Shuttle's systems, the complex networks and devices involved in cybersecurity breaches are interdependent, where the failure of one can lead to dramatic consequences downstream.[49] To better understand the coming wave, from 2013 to 2020, Cisco has estimated that the number of Internet-enabled devices is expected to increase to 50 billion, though estimates vary with Morgan Stanley predicting 75 billion such devices in existence by 2020.[50] Samsung has announced that *all* of its products would be connected to the Internet by 2020.[51] Already, vulnerabilities in such smart devices have been connected with significant security breaches.[52]

The potential wide-ranging impacts of recent cybersecurity breaches into major U.S. corporations cannot be attributed to technical failures alone, as recent examples point toward culture

---

[48] CAIB, *supra* note 35, at 97.

[49] As a recent example, the DDoS attack against Dyn shut down swaths of the Internet by attacking the domain registry. Bruce Schneier, *Lessons from the Dyn DDoS Attack*, SCHNEIER ON SECURITY (Nov. 8, 2016), https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html.

[50] Tony Donava, *Morgan Stanley: 75 Billion Devices Will Be Connected to the Internet of Things By 2020*, BUSINESS INSIDER (Oct. 2, 2013), http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10#ixzz3i4CApJsg.

[51] Rachel Metz, *CES 2015: The Internet of Just About Everything*, MIT TECH. REV. (Jan. 6, 2015), http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything/.

[52] Scott J. Shackelford, *Opinion: How to Fix an Internet of Broken Things,* CHRISTIAN SCIENCE MONITOR (Oct. 26, 2016), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/1026/Opinion-How-to-fix-an-internet-of-broken-things. *See also* Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things*," 2017(2) U. ILL. L. REV. 415, 417–18 (2017) (for an example of hackers causing a car crash).

as being an important element of fault. The 2017 hack of Equifax was the result of a vulnerability the company was warned of prior to the attack.[53] Following their December 2016 breach, Uber, Inc. similarly failed to follow standard industry practices, paying their attacker $100,000 in hush money.[54] More startlingly, Uber kept the exfiltration of millions of customers personal and financial information secret until it was revealed in late 2017.[55] Both of these attacks impacted millions of consumers because of organizational cultures that did not emphasize cybersecurity best practices and industry norms.[56] In fact, Equifax's attempt to hide the extent of their data breach has backfired badly, contributing to proposals to fine credit monitoring firms for such behavior in the future.[57]

Unlike the tragic but relatively low-number of astronaut fatalities that the CAIB investigated, cybersecurity breaches have affected *billions* of people.[58] Analysis of the costs associated with cyber attacks should not stop at the technical failures that allowed the attackers access to the victim's networks. Investigations should take a page from the CAIB's playbook and include

---

[53] *Oversight of the Equifax Data Breach: Answers for Consumers: Hearing Before the Subcomm. on Dig. Commerce & Consumer Prot. of the H. Comm. on Energy and Commerce* (2017) (prepared testimony of Richard F. Smith, CEO and Chairman of the Board, Equifax).

[54] Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, BLOOMBERG (Nov. 21, 2017), https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data. *See also We Investigate: Cyber Crime*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/cyber (recommending against paying a ransom for stolen data, as it only emboldens attackers and potentially funds criminal activity).

[55] Newcomer, *supra* note 54.

[56] *See generally* Scott J. Shackelford et al., *How Businesses Can Promote Cyber Peace*, 36(2) U. PA. J. INT'L L. 353 (2015) (discussing organizational, budgetary, and technological cybersecurity best practices); SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 197–259 (2014) (discussing private sector security) [hereinafter Shackelford, MANAGING CYBER ATTACKS].

[57] *See* Frank Kalman, *Equifax Breach Shows Folly in Hiding Bad News*, TALENT ECONOMY (Sept. 14, 2017), http://www.talenteconomy.io/2017/09/14/equifax-breach-hiding-bad-news/ (discussing the Equifax breach and reactions); Laura Hautala, *Elizabeth Warren's Bill Would Fine the Next Equifax for Data Breach*, CNET (Jan. 10, 2018), https://www.cnet.com/news/elizabeth-warren-equifax-mark-warner-credit-reporting-agencies-data-breach-bill-fines/ (discussing a proposal to fine companies for breaches).

[58] *See World's Biggest Data Breaches*, INFORMATION IS BEAUTIFUL, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (for a graphic identifying the most significant breaches and the extent of their effects).

evaluation of cultural norms that allowed such vulnerabilities to exist, along with industry best practices.[59]

As has been noted, two elements of the NTSB analogy are particularly useful for enhancing cybersecurity. First, it separates fact-finding proceedings from any questions of liability, allowing attribution to be established, for example, without parties initiating litigation.[60] Second is the so-called "party process," which is a multi-stakeholder approach to accident investigations involving members of various constituencies.[61] This multi-stakeholder model is also part and parcel of cybersecurity, and the larger Internet-governance ecosystem,[62] and thus could resonate well with these types of investigations.

The NCSB would likely have significant private-sector participation; in fact, it could even be run entirely by coalitions of companies such as through existing trade groups or Information Sharing and Analysis Centers (ISACs).[63] Moreover, funding could come from interested stakeholders, such as insurance companies.[64] This is because such secondary markets would benefit from greater clarity surrounding the attribution of claims, as well as more information about the utility of various cybersecurity best practices, such as utilizing the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF).[65]

---

[59] *See* Shackelford, MANAGING CYBER ATTACKS, *supra* note 56, at 197–259 (for more discussion of best practices).

[60] Neil Robinson, *The Case for a Cyber-Security Safety Board: A Global View on Risk*, RAND CORP. (June 18, 2012), https://www.rand.org/blog/2012/06/the-case-for-a-cyber-security-safety-board-a-global.html.

[61] *Id.*

[62] *See, e.g.*, Scott J. Shackelford et al., *iGovernance: The Future of Multi-Stakeholder Internet Governance in the Wake of the Apple Encryption Saga*, 42 N.C. J. INT'L L. 883 (2017); Scott J. Shackelford et al., *Back to the Future of Internet Governance?*, 16 GEO. J. INT'L 83 (2015) (for further discussion of Internet governance).

[63] *See Information Sharing,* DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/topic/cybersecurity-information-sharing (for further discussion of information-sharing efforts).

[64] *See* Knake, *supra* note 30 (evaluating the market for cyber insurance).

[65] *See* Scott J. Shackelford et al., *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 223 (2016) (explaining that the NIST Framework "takes a risk-based approach for organizations to detect, mitigate, and respond to cyber threats") [hereinafter Shackelford, *Bottoms Up*]; *see also* Scott J. Shackelford et al., *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L. J. 287, 330 (2015) ("[T]he Cybersecurity Framework 'relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience,' which allows the

Critics of establishing a NCSB would likely contend that firms may spend more on settling litigation and investing in reputation management than in proactively managing cyber attacks.[66] Other concerns might include the fact that as both the cyber threat environment and dependent technologies change so dynamically,[67] the value of NTSB-style investigations may be limited given the concern that, by the time that the investigation is complete, the means used in the data breach may be obsolete. Addressing this concern requires that investigations, once undertaken, are completed as expediently as possible, unlike, for example, the typical NTSB report that can take one year or more to compile.[68] Expediency is more achievable in the cyber-environment, however, because their investigations would not include the time-consuming process of gathering debris and reassembling it that is standard in aviation investigations.[69]

Final concerns that would need to be overcome if the promise of a NCSB is to be realized include: (1) identifying the right experts for the tremendous variety of cyber attacks from Distributed Denial of Service (DDoS) attacks to sophisticated cyber weapons using zero-day exploits;[70] (2) learning from effective information sharing forums to mesh the functions of a NCSB with existing industry best practices and public-private partnerships;[71] (3) defining access (e.g., erring on the side of confidentiality versus transparency for various types of cyber attacks); (4) landing on an appropriate terminology, most likely in the guise of risk management given the success of the NIST CSF[72]; and (5) aligning

---

Framework to 'scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements.'") [hereinafter Shackelford, *Global Standard*].

66 Robinson, *supra* note 60.

67 Andrew Munger, *Reducing Cyberrisk in a Dynamic Threat Environment*, INFRAGARD MAG. (Apr. 1, 2015), https://infragardmagazine.com/how-to-reduce-cyber-risk-in-a-dynamic-threat-environment/.

68 *See The Investigation Process*, NAT'L TRANSP. SAFETY BOARD, https://www.ntsb.gov/investigations/process/Pages/default.aspx (revealing that a proposed report may not go to the Safety Board until 12–18 months from the date of the accident).

69 *Id.* NTSB "Go Teams" include those with "structures" expertise, who "document[ ] airframe wreckage and the accident scene.

70 *See* INTERDISCIPLINARY PATHWAYS, *supra* note 6, at 22 (commenting that the wrong experts will "lead to bad or possibly even harmful, analysis").

71 *See id*. (explaining that the industry has some existing methods for privately sharing information about cyber security incidents that could be used to work more cooperatively).

72 Shackelford, *Bottoms Up*, *supra* note 65, at 243.

efforts with the Federal Trade Commission and other sector-specific regulators to help ensure a more robust cybersecurity standard of care emerges from these efforts.[73] To be successful, a variety of incentives and likely regulatory requirements would be required for firms to participate in a NCSB, such as targeted safe harbor provisions and mandating investigations for "serious" breaches such as those involving U.S. critical infrastructure.[74] It would also be important to limit the purview, and thus workload, of a NCSB given the tremendous number of breaches taking place.

As has been argued by the Cybersecurity Ideas Lab:

> Done right, such an organization could make tremendous contributions, by providing a common base of information about what types of incidents occur, who is affected, who is attacking, the methods of attacks, and the vulnerabilities that are exploited, both at a given point in time and as a way of identifying and characterizing trends.[75]

Such a model would be an improvement on the existing reliance on Cyber Emergency Response Teams (CERTs),[76] and aide in effective policymaking at both the state and federal level given the lack of hard, verifiable data on the scope and scale of cyber attacks. The creation of a NCSB could also help law enforcement investigations, particularly local and state agencies without the resources and expertise of the FBI.[77] Along with the ISACs, this would be a boon to academics needing reliable data to undertake scholarly analysis, as well as national security organizations, and U.S. strategic partners around the world.

III. A GLOBAL NOTE

No nation is an island in cyberspace, as much as some wish they were. As such, jurisdictions the world over are experimenting with

---

[73] Shackelford, *Global Standard*, *supra* note 65, at 320.

[74] *See generally* Scott J. Shackelford et al., *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do About It*, 96(2) NEB. L. REV. 320 (2017) (for further discussion of Russian influence of U.S. elections and other government infrastructure).

[75] INTERDISCIPLINARY PATHWAYS, *supra* note 6, at 21.

[76] *Id.*

[77] *See Police Lack Skills and Funding to Cope with Today's Cyber Threats*, PA CONSULTING (Dec. 12, 2014), http://www.paconsulting.com/newsroom/releases/police-lack-skills-and-funding-to-cope-with-todays-cyber-threats-12-december-2014/ ("only 30% [of police analysts] believe they have the skills and tools to tackle cybercrime effectively").

various cybersecurity risk management models.[78] One of the most important of these jurisdictions is the European Union, both for its overall size,[79] and for the fact that it is undergoing a transformation in its cybersecurity law through the enactment of the General Data Privacy Regulation (GDPR) and the Network Information Security (NIS) Directive.[80] Taken together, these initiatives will revitalize data breach investigations across the European single market with significant implications for global cybersecurity policymaking.[81]

The GDPR—approved by Parliament in 2016—represents the most recent iteration of EU data protection efforts that date back decades.[82] Among other important aspects of the GDPR, it centralizes data protection authority in the EU into a single regulatory body, as compared with the EU Data Protection Directive's (DPD) utilization of national data protection authorities for each Member State.[83] It also mandates breach notification within 72 hours of a covered entity becoming aware of the breach, provides a right to access data to promote the transparency of data privacy, codifies the 'right to be forgotten,' includes a right to data portability, requires privacy by design, and sets out new rules for data protection officers.[84]

Also notable is the shift toward a risk-management model for implementing the privacy principles,[85] a move that may have been influenced by the relative success of the NIST CSF.[86]

---

[78] *See* Shackelford, *Bottoms Up*, *supra* note 65, at 225–26 (describing challenges with the NIST Framework).

[79] *See EU Position in World Trade*, EUROPEAN COMMISSION (Oct. 2, 2014), http://ec.europa.eu/trade/policy/eu-position-in-world-trade/ ("the EU is the biggest player on the global trading scene").

[80] Gabe Maldoff, *NIS + GDRP = New Breach Regime in the EU*, INT'L ASS'N OF PRIVACY PROF. (Dec. 22, 2015), https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/.

[81] Natasja Bolton, *NIS Directive & GDPR: Regulations that Will Have a Global Impact*, SYSNET GLOBAL SOLUTIONS, https://sysnetgs.com/2017/08/nis-directive-gdpr-regulations-will-global-impact/.

[82] *See EU General Data Protection Regulation*, EUGDPR, https://www.eugdpr.org/ (for its homepage).

[83] *Id.; GDPR Key Changes*, EUGDPR, https://www.eugdpr.org/key-changes.html.

[84] *GDPR Key Changes*, *supra* note 83.

[85] *Council of the European Union Proposes Risk-Based Approach to Compliance Obligations*, HUNTON & WILLIAMS PRIVACY & INFO. SECURITY L. BLOG (Oct. 29, 2014), https://www.huntonprivacyblog.com/2014/10/29/council-european-union-proposes-risk-based-approach-compliance-obligations/.

[86] *See* Shackelford, *Bottoms Up*, *supra* note 65, at 236 (discussing the Framework's influence on cybersecurity efforts in Europe); KATHERINE O'KEEFE

> Finally, the GDPR extends the jurisdictional reach of EU data protection requirements to data processing that occurs outside the territorial boundaries of the EU when the processor targets individuals within the EU for the offering of goods or services, or when the processor is monitoring EU persons that are located within the territorial bounds of the EU.[87]

Taken together, these reforms constitute a sea change in the EU's data privacy regime, which is already among the most robust in the world.

In addition to the GDPR, the NIS Directive deepens the EU's reforms by increasing the Member States' cybersecurity capacity-building, defining a "Cooperation Group" to support intra-EU information sharing, and laying out the requirements for operators of "essential services" (analogous to critical infrastructure that includes energy, transportation, banking, financial markets, healthcare, water, and digital infrastructure).[88] Overall, the NIS Directive helps to establish a European standard of cybersecurity care for all businesses based upon risk management.[89]

The above reforms are coupled with a requirement for each EU Member State to enact legislation establishing a national cybersecurity strategy, a national cybersecurity authority, and a national CERT, if such entities do not exist already.[90] The extent of some of these obligations, however, is still unclear, as States may see cyber threats as falling in the realm of national security, and therefore outside the scope of this strata of EU governance.[91] Finally, in furtherance of the emphasis on risk management, crystallizing the EU's Cybersecurity Strategy led to the development of the NIS Platform, which establishes a framework for evaluating cybersecurity due diligence, and which largely

---

& DARAGH O'BRIEN, SUBJECT ACCESS REQUESTS: A DATA HEALTH CHECK 12 ("40% of Data Controllers are failing to ensure adequate technological or organisational controls to prevent unauthorised access to or disclosure of personal data").

87 Scott J. Shackelford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Case Study*, 67 S.C. L. REV. 609, 621 (2016).

88 Council Directive 2016/1148, 2016 O.J. (L 194) 1 (EU).

89 *See* EUR. PARL. DOC. (COM 48) 3.2 (2013) ("[T]he requirements are proportionate to the risk presented . . . and should not apply to micro enterprises.").

90 *Id*. at § 4, 22.

91 *See* Consolidated Version of the Treaty on European Union art. 4, Oct. 26, 2012, 2012 O.J. (C 326) 1 ("national security remains the sole responsibility of each Member state.").

incorporates the NIST CSF core elements—identify, protect, detect, respond, recover—as the standard approach for enterprise risk management.[92]

Looking ahead, the GDPR will automatically come into force across the EU on May 25, 2018, "whereas NISD requires Member States to introduce implementing legislation by 9 May 2018."[93] Once these reforms come into full effect, there will be a flood of information on data breaches across the EU that will help investigators in Europe, North America, and indeed around the world better identify, and hopefully mitigate the risk of, cyber attacks.[94] Although neither the GDPR nor the NIS Directive includes a version of a regional Cybersecurity Safety Board, the elements it does include moves the EU in this direction, which could make an analogous U.S. body that much more effective. Such developments would be an important step on the long journey to a positive and sustainable cyber peace.[95]

CONCLUSION

No system for investigating and reporting on cyber attacks is perfect. Incentives will continue to be misaligned in this context given that many firms fear legal liability and the negative impact on brand that being forthcoming about the details of cyber attacks can bring. But as more nations and regions—including the European Union— join the 47 U.S. states and move forward with more robust data breach notification requirements, a global debate is now underway about the best ways in which to increase transparency and with it, opportunities to learn from successful cyber attacks. A NCSB is politically unlikely in the near term, but we believe that the creation of such a body is overdue.

Without Congressional action, a coalition of the private sector and even state governments could begin the process of enacting local, even sector-specific CSBs. But to reach their full promise (and to ward off wasteful duplication), Congress would need to pass a package of incentives and regulatory requirements outlined

---

[92] NIS PLATFORM (WG1-CHAPTER 1) 14 (Final Draft 220515)

[93] *Data Security and Breach Reporting Under the GDPR and NISD*, TAYLOR WESSING (Sept. 2016), https://united-kingdom.taylorwessing.com/globaldatahub/article-data-security-and-breach-reporting-under-the-gdpr-and-nisd.html.

[94] *See id.* (requiring data controllers to report serious data breaches to the Supervisory Authority within 72 hours).

[95] *See generally* Scott J. Shackelford, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 Stan. L. Rev. 106 (2012) (for more discussion of cyber peace).

above. Although far from a panacea, such a step could help raise the overall level of cybersecurity due diligence and hasten the rise of a cybersecurity standard of care in the United States and abroad. All that is needed is the political will to act, the desire to experiment with new models of cybersecurity governance, and the recognition that we should learn from history. As President Franklin D. Roosevelt famously said: "The country needs and, unless I mistake its temper, the country demands bold, persistent experimentation. It is common sense to take a method and try it: If it fails, admit it frankly and try another. But above all, try something."[96]

[96] Franklin D. Roosevelt, Address at Oglethorpe University (May 22, 1932).