THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON

The Next Step in Federal Cybersecurity? Considering an NTSB-Style Computer Safety Board

June 2018

By Jessica L. Beyer, Drake Birnbaum, and Thomas Zech

Synopsis
In response to the policy proposals for an National Transportation Safety Board-style computer safety board, this report provides a literature review of the major policy proposals for an NTSB-style computer safety board, analyzes the six major components of the NTSB's mandate, and compares these functions to existing federal cybersecurity responsibility. The report also discusses seven major challenges that would need to be addressed to create such a federal computer safety board. The report concludes with four recommendations for the process of creating a computer safety board: (1) map the landscape of federal cybersecurity actors; (2) articulate the need for a computer safety board; (3) clearly scope the mandate, responsibilities, and purview of such a new body to solve issues of focus, liability, and objectivity; and (4) create as much administrative distance for any potential agency from the national security apparatus (e.g., the NSA) as possible.

Contact: Dr. Jessica L. Beyer, Henry M. Jackson School of International Studies, University of Washington, jlbeyer@uw.edu

Table of Contents

Report Summary

As cybersecurity has become an critical issue, the question of how to address it at the federal level has become increasingly pressing. Federal responsibility for cybersecurity is currently distributed across federal agencies, with a complex and sometimes confusing collection of actors responsible for cybersecurity. In light of the ransomware attack that crippled Atlanta in 2018 and the escalating number of cyberattacks across the US, some have proposed the US federal government create an independent computer safety board modeled after the National Transportation Safety Board (NTSB). Most of these arguments focus on the NTSB's investigative mission as a way to conquer issues of information sharing and liability.

In response to the policy proposals for an NTSB-style computer safety board, this report provides a literature review of the major policy proposals for an NTSB-style computer safety board, analyzes the six major components of the NTSB's mandate, and compares these functions to existing federal cybersecurity responsibility.

The report also discusses seven major challenges that would need to be addressed to create such a federal computer safety board. These challenges include the following.

1. The landscape of existing federal cybersecurity responsibility is unclear and makes it difficult to make the case for a computer safety board.
2. The scope and scale of cyberattacks presents challenges for specifying a computer safety board's responsibility.
3. The unique nature of cyber-incidents means that a computer safety board could struggle with defining liability and jurisdiction.
4. The challenges of attribution, specifically determining what is a state-sponsored attack and what is cyber-crime, could also make defining jurisdiction challenging.
5. The involvement of the US government in surveillance and the development of cyber-weapons creates potential objectivity challenges for a computer safety board.
6. Information sharing remains a major cybersecurity issue and could frustrate the investigative efforts of a computer safety board.
7. Without a clearly scoped mandate it is difficult to determine the cost of creating and running a computer safety board.

The report concludes with four recommendations for the process of creating a computer safety board. Based on the research in this report and the existing literature on a computer safety board the report recommends that planners do the following:

1. Map the landscape of federal cybersecurity actors;
2. Articulate the need for a computer safety board;
3. Clearly scope the mandate, responsibilities, and purview of such a new body to solve issues of focus, liability, and objectivity; and
4. Create as much administrative distance for any potential agency from the national security apparatus (e.g., the DoD, NSA, CIA) as possible.

Existing Policy Proposals

There are six major sources that argue for the creation of a computer safety board modeled after the NTSB and one major source that makes the case more generally for a national cybersecurity agency. Most of the sources discussed here share two common elements. First, none of the sources discuss the full range of the NTSB's mandate, instead focusing on its investigative mission, with some minor focus on its standards mandate. Second, most point to the issue of information sharing in cybersecurity investigations as a central reason for creating a third party agency—for most, this addresses questions of liability and data access. This section includes a summary of the major arguments of each of these pieces.

In 2012, Neil Robinson argued that there was a need for a cybersecurity safety board to address issues of information sharing. He argued that a computer safety board that was modeled on the NTSB could serve as an independent third party, as such removing many of the barriers to information sharing. Robinson argued that such a board could work independently from the process of establishing liability and he argued that the multi-stakeholder process that the NTSB uses for investigations, known as the "party process" would be a useful model for a computer safety board.[1]

In 2014, an NSF-sponsored Cybersecurity Ideas Lab report also argued that an NTSB-type investigative organization should be created for cybersecurity incidents — and that its investigations should be kept separate from law enforcement.[2] It also asserted that investigations should be kept independent from organizations responding in the immediate aftermath of an incident and should instead be deep investigations meant to create a public report on what had happened. The task force said that this would be an "improvement upon" the work of the US's Computer Emergency Response Teams (CERTs), although without articulating any CERT problems.[3] The NSF task force cautioned that such a computer safety board would need to address how the right expertise would be assembled for each investigation; how such a board would fit into existing industry practices, pointing to the Information Sharing and Analysis

[1] Robinson, N. (2012). "The Case for a Cyber-Security Safety Board: A Global View on Risk." RAND. June 18, https://www.rand.org/blog/2012/06/the-case-for-a-cyber-security-safety-board-a-global.html
[2] NSF Cybersecurity Ideas Lab. (2014). "Interdisciplinary Pathways Towards a More Secure Internet." February 10-12, https://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf
[3] Ibid, p.21.

Centers (ISACs) and the existing CERTs; how such a body would access data; and how terminology would be standardized, suggesting the use of NIST's frameworks.[4]

In 2016, while making the case for the creation of a federally sponsored cyber insurance program in anticipation of a future catastrophic event in cyberspace, Robert K. Knake argued that because of information sharing issues regulations around investigations would be needed. He asserted that his proposed cyber insurance program would require companies to allow for full investigations of cyber-incidents, including gathering of any data needed, similar to the NTSB and aviation incidents.[5]

In 2016, a Center for Strategic and International Studies (CSIS) report focused on the issue of information sharing in the wake of a cyber-incident. The report asserted that there was a need for victims of a cyberattack to share information anonymously and without concern for liability — in spite of the gains made by the 2015 Cybersecurity Act.[6] The report argued that such a mechanism could be modeled on the NTSB because of the NTSB's rule against using any information submitted to the investigation for enforcement purposes. The CSIS report suggests the DHS or the Cyber Threat Information Integration Center, which is within the Office of the Director of National Intelligence, as future homes for an NTSB-style unit.[7]

In 2018, Scott J. Shackelford and Austin E. Brady picked up many of the recommendations in the 2014 NSF Cybersecurity Ideas Lab report, but broadened the discussion of a computer safety board with a focus the NTSB's investigative mission and issues of information sharing.[8] They also highlighted the difference in scope and scale of cyberattack versus transportation accidents, choosing to focus on space travel as a point of contrast, in particular. Like Robinson and the CSIS report, they also argued that an aspect of the NTSB that is particularly useful when thinking about a computer safety board is the fact that it separates its

[4] NSF Cybersecurity Ideas Lab, 2014, p.22.
[5] Knake, R. K. (2016). "Creating a Federally Sponsored Cyber Insurance Program." Council on Foreign Relations. November 22, https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program
[6] Center for Strategic & International Studies. (2016) "From Awareness to Action: A Cybersecurity Agenda for the 45th President." CSIS Cyber Policy Task Force. January, https://www.whitehouse.senate.gov/imo/media/doc/2016-01-03%20-%20CSIS%20Lewis%20Cyber%20Recommendations%20Next%20Administration.pdf
[7] Ibid, p.12.
[8] Shackelford, S. & Brady, A. (2018). "Is it Time for a National Security Safety Board?" Albany Law Journal of Science and Technology, Kelley School of Business Research Paper No. 18-34. January 12, https://ssrn.com/abstract=3100962

investigative process from any questions of legal liability—allowing investigations to move to conclusion without any litigation. Also like the NSF Cybersecurity Ideas Lab report, Shackelford and Brady highlighted the multi-stakeholder approach that the NTSB takes to accident investigations, pointing to ISACs (and other similar groups) as potential sites of a computer safety board's investigations. They argued that funding for investigations could come from other stakeholders.[9]

Shackelford and Brady also highlight a list of concerns about an NTSB-style computer safety board, including: considering that technology changes quickly so investigations would need to happen quickly; considering the complexity of attacks, finding the right experts would be a challenge; considering the barrier that information sharing poses, close study of information sharing organizations would need to happen and clear parameters of data access would need to be created; considering the issues with terminology, standards would need to be created; and any computer safety efforts align with the Federal Trade Commission and sector-specific regulators. Shackelford and Brady also noted the European Union's (EU) General Data Protection Regulation (GDPR) GDPR's risk management model could be a valuable approach.[10]

Paul Rosenzweig's 2018 discussion of a potential computer safety board also centered on the NTSB's investigative mission and, to some limited extent, on its role as a safety standards issuer. Within these parameters, Rosenweig argued that a computer safety board modeled after the NTSB should do the following: focus on risk reduction rather than elimination, acknowledge the scope and scale of cyber-attack and create a threshold for review, acknowledge that attribution is difficult in cyber-incidents, recognize that systems are always vulnerable so there is no perfect defense, acknowledge the issues with cooperation, and structure any computer safety board with an understanding that humans and technology are the cause of cybersecurity breaches.[11]

Although not focused on an NTSB-style computer safety board, Microsoft's February 2018 recommendation for a "national cybersecurity agency" dovetails with some of the

[9] Shackelford & Brady, 2018, p.12.
[10] Ibid, p.15.
[11] Rosenzweig, P. (2018). "The NTSB as a Model for Cybersecurity." R Street. May, https://2o9ub0417chl2lg6m43em6psi2i-wpengine.netdna-ssl.com/wp-content/uploads/2018/05/Final-Short-No.-58.pdf

recommendations for a computer safety board.[12] Microsoft argues that a single cybersecurity agency should be created at the federal level that manages civilian agencies, critical infrastructure protection, and incident response as well as putting forth best practice recommendations. Microsoft's white paper asserts that such an agency would need a clear mandate and appropriate statutory powers because it would be navigating a dense web of other government agencies, legislative arms, regulatory bodies, civil society groups, citizens, and any other number of organizations. The report also makes recommendations about the form of such an agency, including that it have a policy and planning unit, an outreach and partnership unit, a communications unit, an operations unit that acts like a CERT, and a regulatory unit.

[12] Report is attached to the blog post - Microsoft Corporation (2018). "Building a National Cybersecurity Agency." Microsoft Policy Papers. February 19, https://cloudblogs.microsoft.com/microsoftsecure/2018/02/19/how-a-national-cybersecurity-agency-can-help-avoid-a-national-cybersecurity-quagmire/

NTSB Core Functions and Cybersecurity Responsibilities

Most people proposing an NTSB-style computer safety board focus on the NTSB's investigative process; however, the NTSB has six core functions. This section separates the NTSB's six functions and describes each and then discusses the parallel cybersecurity responsibilities within these categories.

The NTSB has six core functions it is legislatively mandated to oversee: maintaining independence and objectivity, conducting objective accident investigations and safety studies, performing fair airman and mariner certification appeals, promoting safety recommendations, and transportation accident assistance.[13] For the purposes of this analysis, we split these into the following categories and discuss each in turn:

- Maintaining independence and objectivity
- Investigating accidents
- Conducting safety studies and promoting recommendations
- Performing certification appeals
- Assisting the victims of accidents
- Training

Maintaining Independence and Objectivity

The NTSB's independence and objectivity are two of the agency's core characteristics; however, these characteristics would be difficult to emulate unless a computer safety board's mandate was scoped very precisely to articulate what responsibilities were being taken from other agencies and what organizations held authority. When independence and objectivity are discussed in the works cited in the literature review, it is nearly always in relation to liability, rather than independence from other agencies.

NTSB: Independence and Objectivity

The NTSB is an independent federal agency with no ability to either regulate or be otherwise directly involved in transportation operations.[14] Although it began as a subsidiary of

[13] National Transportation Safety Board. "Fiscal Years 2018-2022 Strategic Plan." NTSB.gov. Accessed June 11, 2018 at https://www.ntsb.gov/about/reports/Documents/FY2018-2022strategicPlan.pdf. p6.
[14] National Transportation Safety Board, 2018.

the Department of Transportation, in the 1970s it was given complete independence—allowing it to operate outside the influence of other federal entities.

The NTSB is run by a five member board made up of Presidential nominees who the Senate approves. No more than three of these members can be from the same political party. Two of them are nominated by the President to serve as the Chairman and Vice Chairman of the NTSB. The NTSB also includes 13 other offices each tasked with elements of the NTSB's mission.[15]

Cybersecurity: Independence and Objectivity

Currently, federal cybersecurity responsibility is divided across agencies making cybersecurity oversight the opposite of independent. The web of responsibility is convoluted and there are few existing sources that pull apart different areas of responsibility from the macro to the micro level.[16] Every agency must provide for its own cybersecurity[17]—but there are actors that serve in cross-organizational roles. The landscape means that there is no single place that holds responsibility for incident response and investigation, let alone the other duties a computer-focused safety board might have.

In 2018, Katherine Charlet produced a report in which she characterized the macro-level cybersecurity relationships as: (1) the Office of Management and Budget puts forth government wide policies; (2) NIST puts forth the standards for other agencies that are both mandatory and guidelines; (3) the various agencies put the policies, standards, and guidelines into place; (4) the DHS provides "operational direction, assistance, and technical capability to help" with this adoption; (5) the General Services Administration helps actors in acquiring any cybersecurity services or products; (6) and the Office of Management and Budget then monitors this process reporting on implementation.[18] Charlet acknowledges that DoD, the intelligence community, and

---

[15] National Transportation Safety Board. (2016). "Organizational Chart." NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/about/organization/Documents/ntsb-org-chart-2016.pdf

[16] An exception is the work of Chartlet (2018), which makes a noble effort to parse out this complicated landscape. Although this examines agency responsibility at the macro level (e.g., DHS) without a close look at lower levels (e.g., CERTs) or external organizations deeply involved in cybersecurity (e.g., ISACs). She also looks at major policies. Charlet, K. (2018). "Understanding Federal Cybersecurity." Paper, Cyber Security Project, Harvard University Belfer Center. April, https://www.belfercenter.org/publication/understanding-federal-cybersecurity

[17] Federal Information Security Modernization Act of 2014. Public Law 113-283. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf16.

[18] Charlet, 2018. See p10 for a wonderful flow chart.

the FBI also provide key cybersecurity support, as the FBI would lead any investigation into breaches or attacks and the DoD and the intelligence community would be on the front lines of response—including national security. Charlet also cites the US Digital Services as important as well as it has teams within agencies that provide support for cost saving measures and the provision of "bug bounties."[19]

However, not discussed by Charlet is that within each of these major bodies, there is a wide range of mezzo and micro-level actors with important cybersecurity functions. For example, the DHS oversees critical infrastructure—making it a core actor in domestic cybersecurity protection. But, within the DHS the 16 critical infrastructure designations contain a vast amount of the US's cyber-physical infrastructure protected by DHS—and each designation has different configurations of stakeholders involved in cyber-physical protection. The Government Facilities Sector[20] is a good example of the range of infrastructure that can be contained under one critical infrastructure plan, containing everything from schools to electoral systems.[21]

In addition, to protect domestic infrastructure, the DHS supports a range of organizations—such as the National Cybersecurity and Communications Integration Center (NCCIC). The National Cybersecurity and Communications Integration Center houses several organizations central to cybersecurity, notably the US-CERT[22] and the ICS-CERT.[23] Both the US-CERT and the ICS-CERT share the NCCIC's mission of serving as a global resource for cybersecurity information—including risk assessment, education, and general support.[24] The NCCIC also is tasked with defending federal networks and responding to major incidents. The NCCIC defines its mission as information exchange, training and exercises, risk and vulnerability assessments, data synthesis and analysis, operational planning and coordination, watch operations, and incident response and recovery—a list that sounds similar to the NTSB's

[19] Ibid, p13.
[20] Department of Homeland Security. (n.d.). "Government Facilities Sector." DHS.gov. Accessed June 25, 2018 at https://www.dhs.gov/government-facilities-sector
[21] Department of Homeland Security. (2015). "Government Facilities Sector-Specific Plan." DHS.gov. Accessed June 25, 2018 at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf
[22] US-CERT website. (n.d.). Accessed June 25, 2018 at https://www.us-cert.gov/
[23] ICS-CERT website. (n.d.). Accessed June 25, 2018 at https://ics-cert.us-cert.gov/
[24] This mission is listed on both the US-CERT and the ICS-CERT websites.

mission.[25] In that work, the NCCIC may work closely with the FBI to uncover threats, as does the NTSB.[26]

Investigating Accidents

The NTSB's investigative model was the central element in nearly every policy proposal for a computer safety board modeled on the NTSB.[27] However, potential complicating factors in using this part of the NTSB as a model is that the incident response function similar to that of the NTSB already exists spread across other organizations and, as mentioned, cyberattack is more frequent than the type of transportation accidents that the NTSB investigates.

NTSB: Investigating Accidents

The NTSB investigations are comprised of "Go Teams" these teams can number from three to a dozen specialists from the Board's headquarters and respond as quickly as possible to the scene of an accident.[28] These teams contain the necessary experts to examine the scene of an accident and determine cause. During investigations, the NTSB may issue safety recommendations as a result of findings. The NTSB may also hold public hearings as part of its investigation. Once an investigation is completed, the NTSB takes the findings of the investigative team and writes a final report. This report is deliberated in public and is ultimately published on the NTSB website.[29]

The NTSB investigates around 2,000 aviation incidents a year and about 500 other types of accidents from railway, highway, marine, and pipeline accidents. In order to do this with around 400 employees, the NTSB can designate other organizations and companies as parties to its investigations—what the NTSB calls the "party system." The NTSB can designate any entity it wants to as a party to an investigation. Any designated party must provide some needed

---

[25] Ibid, n.d.
[26] US-CERT. (n.d.). "HIDDEN COBRA - North Korean Malicious Cyber Activity." us-cert.gov. Accessed June 25, 2018 at https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
[27] This includes Robinson (2012), the Cybersecurity Ideas Lab report (2014), Knake (2016), the CSIS report (2016), Shackelford and Brady (2018), and Rosenzweig (2018).
[28] National Transportation Safety Board. "The Investigative Process." NTSB.gov. Accessed June 11, 2018 at https://www.ntsb.gov/investigations/process/Pages/default.aspx.
[29] National Transportation Safety Board. "The Investigative Process."

expertise to an investigation. Each investigative group produces reports of the investigations that become public record.[30]

The NTSB also has the mandate to provide assistance in criminal investigations—although in cases of crime, the NTSB has no jurisdiction and must give any investigation over to the relevant law enforcement agency. The NTSB also assists other domestic agencies as appropriate and can assist foreign governments in the cases of air accidents. The NTSB also may offer assistance to governments without the necessary technical expertise to investigate accidents.[31]

Cybersecurity: Investigating Accidents

There are two major complications with replicating this core mission of the NTSB in a cybersecurity safety board. First, the number of cyberattacks is massive and it would be difficult to decide which attacks should be the responsibility of a computer safety board. Second, investigative capability already exists in other federal agencies and due to the nature of cyber-incidents, it is challenging to parse where authority should lie.

The number of cyberattacks that occur daily dwarfs the number of accidents—even combined across the many arenas the NTSB has authority to oversee. The NTSB reports that it investigates close to 2,000 aviation incidents a year and around 500 other types of accidents.[32] However, companies such as Microsoft report grappling with up to a million cyberattacks a day.[33] Microsoft executives discuss having to use machine learning to update counter-measures multiple times a day because of the scope and scale of attack.[34] While the NTSB does not investigate every accident and a computer safety board would likely not address every cyberattack, a very detailed criteria would have to be generated to determine what type of attack a computer safety board would have authority to investigate. This would also mean delineating

[30] Ibid, n.d.
[31] Ibid, n.d.
[32] Ibid, n.d.
[33] Microsoft Corporation. (2015). "PLATINUM: Targeted attacks in South and Southeast Asia." Microsoft Security Intelligence Report, v. 20. July-December, https://www.microsoft.com/en-us/download/details.aspx?id=52255 p.vi.
[34] Marzouk, Z. (2017). "Microsoft Sees 300% Increase in Cyber Attacks in the Last Year." ITPRO.co.uk. October 4, http://www.itpro.co.uk/security/29632/microsoft-sees-300-increase-in-cyber-attacks-in-the-last-year

out what an entity such as the US-CERT should have authority to handle versus a computer safety board.

Investigative duties for cyberattacks exist in other federal agencies. According to an Obama-era directive, the Presidential Policy Directive-41, the FBI and the Department of Justice's National Cyber Investigative Task Force are the lead in response to cyberattack. The NCCIC is designated to provide backup. PPD-41 also contains a definition of "significant" cyberattack and what a cyber-incident is.[35]

Conducting Safety Studies and Promoting Recommendations

The NTSB not only works to determine the cause of major accidents, but also conducts safety studies and promotes safety recommendations. A potential complication for incorporating this element of the NTSB into a computer safety board is that NIST, within the Department of Commerce, already acts as the major cybersecurity standards entity for the federal government. In addition, many other actors also put out safety recommendations.

NTSB: Conducting Safety Studies and Promoting Safety Recommendations

The NTSB's safety recommendations come from incident investigations and from evaluations of the effectiveness of other government agencies' programs. They are also derived from the review of any appeals that the NTSB hears around the removal of aviation and mariner FAA and Coast Guard issued certifications.

When the NTSB concludes an incident or other type of investigation, it issues safety recommendations to the entire body of stakeholders, including government at all levels, industry, and any organization involved in transportation safety. These safety reports are also stored on the NTSB's website, in many cases.[36]

---

[35] Obama, B. (2016). "Presidential Policy Directive — United States Cyber Incident Coordination." White House: Office of the Press Secretary. Accessed June 25, 2018 at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[36] National Transportation Safety Board. (n.d.). "Safety Advocacy." NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/safety/Pages/default.aspx

Cybersecurity: Conducting Safety Studies and Promoting Safety Recommendations

The policy pieces that make the recommendation that a computer safety board be created modeled on the NTSB's investigative function often also argue that new safety board issue safety and other guidelines on the basis of its cyber-incident investigations. Currently, the Department of Commerce houses the National Institute of Standards and Technology (NIST), which is one of the major standards producing agencies in the federal government, issuing federal cybersecurity frameworks that outlines standards, guides, and risks for the federal government[37]—among many other cybersecurity related standards and resources.[38] Although NIST is the major cybersecurity safety standard provider for the government and the Trump Administration has made all agencies responsible for adopting NIST's Cybersecurity Framework,[39] it is not the only one. The US-CERT,[40] GAO,[41] FCC,[42] FDA,[43] FTC,[44] and others issue cybersecurity guidance and education to the government and the public as well.

Performing Certification Appeals

Another important NTSB function—but one that is rarely mentioned in policy proposals related to a computer safety board—is the NTSB's role in performing certification appeals. Unlike the area of physical transportation, cybersecurity certifications lie with a wide range of organizations.

---

[37] National Institute of Standards and Technology. (2018). "Cybersecurity Framework." NIST.gov. Accessed June 25, 2018 at https://www.nist.gov/cyberframework
[38] National Institute of Standards and Technology. (n.d.). "Computer Security Resource Center." NIST.gov. Accessed June 25, 2018 at https://csrc.nist.gov/
[39] National Institute of Standards and Technology, "Cybersecurity Framework."
[40] US-CERT. (n.d.). "Tips." US-CERT.gov. Accessed June 25, 2018 at https://www.us-cert.gov/ncas/tips
[41] U.S. Government Accountability Office. (n.d.). "Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information - High Risk Issue." GAO.gov. Accessed June 25, 2018 at https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary
[42] Federal Communications Commission. (2018). "Cybersecurity Tips for International Travelers." FCC.gov. March 28, https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers
[43] USDA. (2018). "Medical Devices: Cybersecurity." FDA.gov. April 17, https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
[44] Federal Trade Commission. (n.d.). "Data Security." FTC.gov. Accessed June 25, 2018 at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

NTSB: Performing Certification Appeals

The NTSB hears appeals from mechanics, airmen, mariners, and other aviation-related companies who have had their certification revoked by the Federal Aviation Administration or the Coast Guard. Appeals are heard by a set of administrative law judges whose judgements may be appealed again to either the NTSB's board or through the federal court system.[45]

Cybersecurity: Performing Certification Appeals

Currently, cybersecurity certifications reside with educational, professional, and commercial entities—which provide them in response to a variety of processes. There is no federal agency responsible for all inclusive certification.

Assisting the Victims of Accidents

The NTSB's mandate also includes providing comprehensive support for victims of a major transportation disaster. Due to the difficulty in assigning blame for cyber-incidents and the role that companies play in response to cyberattacks, it would be difficult to incorporate this element of the NTSB into a computer safety board.

NTSB: Assisting the Victims of Accidents

Within the NTSB, the Transportation Disaster Assistance Division (TDA) is the entity responsible for coordinating disaster response across all agencies at all levels, including government and volunteer organizations. The TDA not only offers operational support, but provides information to family members following an accident, as well as family counseling, victim identification and forensic services, communicating with foreign governments, and translation services, among other services.

In the support of accident victims, the NTSB works with other federal agencies, including the Department of State, the Department of Health and Human Services, the FBI, DHS, and DoD. The NTSB also works with the American Red Cross.[46]

---

[45] National Transportation Safety Board. (n.d.). "Administrative Law Judges." NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/legal/alj/Pages/default.aspx

[46] National Transportation Safety Board. (n.d.). " Family Assistance Operations: Planning and Policy." NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/tda/ops/Pages/default.aspx

Cybersecurity: Assisting the Victims of Accidents

Assistance to the victims of cyberattack is also fragmented, making a cohesive computer safety board response difficult. There is a range of financial institution-based responses to identity and credit card theft as well as cybersecurity insurance for larger actors. Additionally, responses to major cyber-incidents often fall to the company whose product was exploited in the attack. However, these companies usually have fairly robust liability protection, as does the US government in the case of one of its cyber-weapons, such as Eternal Blue, being used in attacks, so it may be difficult to compel major stakeholders to assist in victim response.[47]

Training Courses

The NTSB also provides a suit of training courses through the Transportation Disaster Assistance Division (TDA). There is no similar centralized location for such training within cybersecurity.

NTSB: Training Courses

TDA provided courses include courses in family assistance for actors who may find themselves in a position to support families in the wake of an accident; courses for emergency responders needing to learn how to manage a transportation disaster; courses for medical-legal professionals who may need to manage a mass fatality incident; and a course for communities needing to manage mass fatality transportation accidents.[48]

Cybersecurity: Training Courses

Much like professional certifications, there is no centralized location for cybersecurity courses, although considering the vulnerability of small and medium sized businesses in the US

[47] Wolfe, J. (2017). "Cyber attack could spark lawsuits but not against Microsoft." Reuters.com. May 15, https://www.reuters.com/article/us-cyber-attack-liability/cyber-attack-could-spark-lawsuits-but-not-against-microsoft-idUSKCN18B2SE

[48] National Transportation Safety Board. (n.d.). " Information for Emergency Responders, Government Agencies, and Public Safety Personnel." NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/tda/er/Pages/default.aspx

to the hazardous repercussions of cyberattack,[49] it might be critical for the 60% of them that go out of business after an attack.[50]

[49] Liwer, D. (2018). "4 main reasons why SMEs and SMBs fail after a major cyberattack." csoonline.com. April 2, https://www.csoonline.com/article/3267715/cyber-attacks-espionage/4-main-reasons-why-smes-and-smbs-fail-after-a-major-cyberattack.html

[50] Aguilar, L. A. (2015). "The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses." U.S. Securities and Exchange Commission. October 19, https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Challenges for an NTSB-style Computer Safety Board

There are seven major challenges that should be discussed in relation to a computer safety board: (1) the barrier of an unclear landscape of existing cybersecurity responsibility, (2) the challenge of the scope and scale of cyberattacks, (3) the issue of the unique nature of cyber-incidents, (4) the difficulties of attribution, (5) the problem of agency objectivity, (6) the pitfalls surrounding information sharing, and (7) the cost of creating a computer safety board.

Issue 1: Unclear Landscape of Existing Cybersecurity Responsibility

It is unclear how a new cybersecurity organization would fit into the overall landscape of federal cybersecurity responsibility. We found a limited number of resources that contain a full landscape analysis of all federal organizations responsible for cybersecurity outside of Charlet's work, one National Governors Association report, and an older GAO report.[51] None of the literature cited in this report that argues for an NTSB-style computer safety board engages in any detailed discussion of who is responsible for what and where overlap exists. For example, the Cybersecurity Ideas Lab's report argues that a computer safety board could make up for the shortcomings of the CERTs, without ever providing evidence of shortcomings or offering any insight into how such a safety board would overlap with the CERTs.[52] This type of detail haziness in detail is reproduced across most of the sources arguing for a computer safety board.

Issue 2: The Scope and Scale of Cyberattacks

As mentioned previously, the scope and scale of cyberattacks in relation to physical accidents is quite different—something Shackelford and Brady[53] and Rosenzweig also note. In addition, cyberattacks are constant and range from individual level attacks, such as credit card

[51] Charlet, 2018; National Governors Association. (2014). "Federal Cybersecurity Programs: A Resource Guide." NGA.org. Accessed June 25, 2018 at https://www.nga.org/files/live/sites/NGA/files/pdf/2014/1410FederalCybersecurityPrograms.pdf ; Government Accountability Office. (2013). "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." GAO.gov. February, https://www.gao.gov/assets/660/652170.pdf - findings from this report were visualized here - Dorado, E. and O'Sullivan, A. (2015). "Dozens of Federal Cybersecurity Offices Duplicate Efforts with Poor Coordination." George Mason University's Mercatus Center blog. April 14, https://www.mercatus.org/publication/dozens-federal-cybersecurity-offices-duplicate-efforts-poor-coordination

[52] Cybersecurity Ideas Lab, p.21.

[53] Shackelford and Brady, p15.

fraud or identity theft, to state-level attacks, such as the Russian attacks on the US elections. In between are attacks such as WannaCry, which used a leaked NSA cyber-weapon to exploit most versions of Windows and was likely sponsored by a hostile nation-state,[54] to attacks such as the ransomware attack on the city of Atlanta,[55] which was likely the action of a known criminal enterprise, to the botnet attack on Dyn,[56] which was wrapped up in an attempted gaming scam. The sheer variability of attack-type and scale makes any single policy or solution impossible—making the creation of a computer safety board a complex undertaking that would require work to scope the new safety board's mandate very clearly.[57]

Issue 3: The Unique Nature of Cyber-Incidents

The underlying causes of cyber-incidents and the location of liability in a cyber-incident is different than that of transportation accidents, presenting an NTSB-style computer safety board with some serious challenges. The vast majority of cyber-incidents are caused by a combination of: (1) software that has some vulnerability, (2) malicious software created by someone to exploit that vulnerability, and (3) human error. Vulnerable software and human error as causes for a cyber-incident are similar to the accidents that the NTSB investigates—where something such as faulty wiring may lead to a plane crash or a train driver asleep at the wheel may cause a major train accident. But, most cases of cyber-incident are the result of a criminal creating malware or engaging in some other criminal act. In the case of transportation accidents, when criminal action is involved the NTSB hands the investigation over to the appropriate law enforcement agency. In the case of a cyberattack investigation, in order to have any jurisdiction a computer safety board would have to be given authority to investigate the underlying crime—malware and the actors that created it—rather than passing it off to law enforcement.

---

[54] Reuters. (2017). "U.S. blames North Korea for 'WannaCry' cyber attack." Reuters.com. December 18, https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

[55] Blinder, A. and Perlroth, N. (2018). "A Cyberattack Hobbles Atlanta, and Security Experts Shudder." New York Times. March 27, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

[56] Graff, G. (2017). "How a Dorm Room Minecraft Scam Brought Down the Internet." Wired Magazine. December 13, https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

[57] Rosenzweig, 2018, p2 also acknowledges the need to create some kind of criteria for determining cyber-incidents to be investigated.

Additionally, industry is currently responsible for defending against most cyberattacks, investigating the causes of those attacks, and fixing the vulnerabilities that allowed for attacks to occur. Most industry executives do not want the federal government's involvement in their products, particularly post-Snowden—although many companies are willing to cooperate with the government and each other to solve difficult cybersecurity issues. Therefore, unlike the NTSB's party system, which designates experts in response to an incident, technology companies would need to be major stakeholders in any computer safety board from the start.

Issue 4: Attribution is Difficult

Because any nation-state sponsored attack would likely need to remain the purview of the Department of Defense, the challenges of attribution mean that it would also be quite difficult to determine what constitutes a nation-state sponsored incident and what constitutes cyber-crime. A good example of this is the WannaCry attack, which has now been attributed to North Korean hackers. As Rosenzweig points out, attribution in cyber-incidents is not as clear cut or as determinative as it is in incidents such as a train accident.[58]

Issue 5: The Problem of Agency Objectivity

It is also important to note that objectivity as a concept is deeply problematic when discussing federal cybersecurity because of the work of the NSA and CIA. The US government is a known actor in the offensive cyber-weaponry race, and while this work is confined to certain parts of the US government, the use of everyday software used by normal people around the world to create cyber-weapons makes the federal government suspicious to industry and other actors. Even well-respected organizations such as the US-CERT could be viewed as inherently biased. In addition, the secretive nature of the DoD, CIA, and NSA mean that it is possible for the US to be subject to the same cyber-weapon that have been developed for offensive purposes without the DHS knowing what the origin of the attack is—as was the case with Stuxnet.

Therefore, while the DHS might appear to be the natural home for any new computer safety board, as the CSIS report argued[59]—or a beefed up NCCIC that serves that purpose—it would probably not be perceived as objective or independent. In addition, the type of data that

[58] Rosenzweig, 2018, p2.
[59] Center for Strategic & International Studies, "From Awareness to Action: A Cybersecurity Agenda for the 45th President," p12.

investigators might gain access to in an incident investigation would amplify concerns about objectivity.

Issue 6: Information Sharing Challenges

Information sharing is consistently listed as one of the major contemporary cybersecurity challenges. While the DHS houses many organizations meant to facilitate information sharing, including the sector plans tied to the 16 areas of critical infrastructure and the ISAO umbrella, information sharing remains spotty and industry specific. Some ISACs, such as the financial ISAC, are often cited as being fairly effective in sector information sharing—while others are not.[60] Within industry, lack of trust frustrates information sharing as does concerns over intellectual property, liability,[61] and reputation loss.

Additionally, the relationship between industry and government continues to be tense when it comes to information sharing in spite of the 2015 Cybersecurity Act. In the wake of Snowden's revelations, many governments, consumers, and other organizations believe that the relationship between US-based technology companies and the US government is too close, causing industry to distance itself from the US government. Industry continues to express frustration with US government's practice of stockpiling vulnerabilities and creating offensive cyber-weaponry using products created by companies and used by large numbers of people. The pushback against the US government because of incidents such as the loss of Eternal Blue is increasing, as the example of the Microsoft-created Cybersecurity Tech Accord illustrates.[62]

Issue 7: Funding a Computer Safety Board

The cost of a computer safety board is difficult to predict without understanding the scoping of such a safety board. But, for comparison, the NTSB requested a budget of $106 million in 2017.[63]

---

[60] Beyer, personal conversations.

[61] The issue of liability was also pointed out by Robinson (2012), CSIS report (2016), Shackelford and Brady (2018), and Rosenzweig (2018).

[62] Volz, D. (2018). "Tech firms, including Microsoft, Facebook, vow not to aid government cyber attacks." Reuters.com. April 17, https://www.reuters.com/article/us-usa-cyber-microsoft/tech-firms-including-microsoft-facebook-vow-not-to-aid-government-cyber-attacks-idUSKBN1HO283

[63] National Transportation Safety Board. (2016). "National Transportation Safety Board Fiscal Year 2017 Budget Request." NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/about/reports/Documents/NTSB_FY2017_Budget.pdf

Recommendations

This report makes four major recommendations for proceeding with a policy proposal for an NTSB-style computer safety board based on both the independent research conducted for this report and the existing literature on a computer safety board: (1) map the landscape of federal cybersecurity actors; (2) articulate the need for a computer safety board; (3) clearly scope the mandate, responsibilities, and purview of such a new body to solve issues of focus, liability, and objectivity; and (4) create as much administrative distance for any potential agency from the national security apparatus (DoD, NSA, CIA) as possible.

Recommendation 1: Map the Landscape of Federal Cybersecurity Actors

Without a landscape analysis that covers all elements of federal cybersecurity organization, policy, and associated organizations, it is impossible to understand where a computer safety board would exist in the overall federal organizational structure; whether such a board is needed or if an existing organization could be given more resources, autonomy, and responsibility; and what kinds of turf wars might erupt if such a computer safety board were created.

Recommendation 2: Articulate the Need for a Computer Safety Board

The second recommendation is that once a landscape analysis was completed, a case should be made for how a computer safety board would interact and replace existing actors within the federal cybersecurity arena. The current literature proposing such a board points nearly exclusively to the NTSB's investigative mission and occasionally its production of safety standards, without deeply engaging with whether the same functions exist elsewhere. It is unclear from existing policy proposals what the need for a new organization is in the overall landscape.

Recommendation 3: Clearly Scope the New Organization

Many of the potential pitfalls for a computer safety board listed in this report—including the scope and scale of cyberattacks, the unique nature of cyber-incidents, the issues with attribution and agency objectivity, and information sharing challenges—and issues discussed in other policy proposals focus on issues that could be solved with clear scoping of the mandate,

responsibilities, and purview of the new board. In the planning stages of this organization, proposers would need to specify a framework for what types of attacks were the responsibility of the computer safety board to solve the issue of the scope and scale of cyberattacks.

Proposers would need to address the issue of liability—giving stakeholders assurances that information shared would not lead to greater liability and that the companies making vulnerable products and the humans making errors were not ultimately liable for cyber-incident. However, this would present a new issue in that proposers would need to decide how to address the issue of whether such a computer safety board would be able to investigate crime, unlike the NTSB, since nearly all cyber-incidents are the result of malicious action.

Finally, proposers would need to attempt to solve the issue of objectivity—particularly in light of the US government's continued engagement in the international cyber-weapon race. Whether one believes that the development of offensive cyber-weaponry is necessary for national security or not, its continuation creates a challenge for the industry-government information sharing and trust needed to collaborate in any cooperative cyber-incident investigation.

Recommendation 4: Create Administrative Distance

Finally, tied to the issue of objectivity, any potential agency should be given as much distance from the national security apparatus as possible. The US government is a known actor in the offensive cyber-weaponry race, and while this work is confined to certain parts of the US government, the use of everyday software used by normal people to create cyber-weapons is a fundamentally different phenomenon than the creation of the kinetic weaponry that may target airplanes, roads, boats, or trains. The recent use of US government cyber-weapons in other major cyberattacks has only heightened tensions between the US federal government and other actors. The only way to address this issue is to give any potential agency as much regulatory distance and autonomy from the Department of Defense and the intelligence community as possible.

Sources

Aguilar, L. A. (2015). "The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses." U.S. Securities and Exchange Commission. October 19, https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Blinder, A. and Perlroth, N. (2018). "A Cyberattack Hobbles Atlanta, and Security Experts Shudder." New York Times. March 27, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

Center for Strategic & International Studies. (2016) "From Awareness to Action: A Cybersecurity Agenda for the 45th President." CSIS Cyber Policy Task Force. January, https://www.whitehouse.senate.gov/imo/media/doc/2016-01-03%20-%20CSIS%20Lewis%20Cyber%20Recommendations%20Next%20Administration.pdf

Charlet, K. (2018). "Understanding Federal Cybersecurity." Paper, Cyber Security Project, Harvard University Belfer Center. April, https://www.belfercenter.org/publication/understanding-federal-cybersecurity

Department of Homeland Security. (n.d.). "Government Facilities Sector." dhs.gov. Accessed June 25, https://www.dhs.gov/government-facilities-sector

Department of Homeland Security. (2015). "Government Facilities Sector-Specific Plan." dhs.gov. Accessed June 25, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf

Dorado, E. and O'Sullivan, A. (2015). "Dozens of Federal Cybersecurity Offices Duplicate Efforts with Poor Coordination." George Mason University's Mercatus Center blog. April 14, https://www.mercatus.org/publication/dozens-federal-cybersecurity-offices-duplicate-efforts-poor-coordination

Federal Communications Commission. (2018). "Cybersecurity Tips for International Travelers." FCC.gov. March 28, https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers

Federal Information Security Modernization Act of 2014. Public Law 113-283. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf16.

Federal Trade Commission. (n.d.). "Data Security." FTC.gov. Accessed June 25, 2018 at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

Government Accountability Office. (2013). "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." GAO.gov. February, https://www.gao.gov/assets/660/652170.pdf

Graff, G. (2017). "How a Dorm Room Minecraft Scam Brought Down the Internet." Wired Magazine. December 13, https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

ICS-CERT website. (n.d.). Accessed June 25, 2018 at https://ics-cert.us-cert.gov/

Knake, R. P. (2016). "Creating a Federally Sponsored Cyber Insurance Program." Council on Foreign Relations. November 22, https://www.cfr.org/report/creating-federally-sponsored-cyber-insurance-program.

Liwer, D. (2018). "4 main reasons why SMEs and SMBs fail after a major cyberattack." csoonline.com. April 2, https://www.csoonline.com/article/3267715/cyber-attacks-espionage/4-main-reasons-why-smes-and-smbs-fail-after-a-major-cyberattack.html

Marzouk, Z. (2017). “Microsoft Sees 300% Increase in Cyber Attacks in the Last Year.” ITPRO.co.uk. October 4, http://www.itpro.co.uk/security/29632/microsoft-sees-300-increase-in-cyber-attacks-in-the-last-year

Microsoft Corporation (2018). “Building a National Cybersecurity Agency.” Microsoft Policy Papers. February 19, https://cloudblogs.microsoft.com/microsoftsecure/2018/02/19/how-a-national-cybersecurity-agency-can-help-avoid-a-national-cybersecurity-quagmire/

Microsoft Corporation. (2015). “PLATINUM: Targeted attacks in South and Southeast Asia.” Microsoft Security Intelligence Report, v. 20. July-December, https://www.microsoft.com/en-us/download/details.aspx?id=52255

Mundal, E. (2018). “Is It Time for a NTSB-Style Cybersecurity Board?” Inside Sources. May 13, http://www.insidesources.com/is-it-time-for-an-ntsb-style-cybersecurity-board/

National Governors Association. (2014). “Federal Cybersecurity Programs: A Resource Guide.” NGA.org. Accessed June 25, 2018 at https://www.nga.org/files/live/sites/NGA/files/pdf/2014/1410FederalCybersecurityPrograms.pdf

National Institute of Standards and Technology. (n.d.). “Computer Security Resource Center.” NIST.gov. Accessed June 25, 2018 at https://csrc.nist.gov/

National Institute of Standards and Technology. (2018). “Cybersecurity Framework.” NIST.gov. Accessed June 25, 2018 at https://www.nist.gov/cyberframework

National Transportation Safety Board. (n.d.). “Administrative Law Judges.” NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/legal/alj/Pages/default.aspx

National Transportation Safety Board. (n.d.). “ Family Assistance Operations: Planning and Policy.” NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/tda/ops/Pages/default.aspx

National Transportation Safety Board. "Fiscal Years 2018-2022 Strategic Plan." NTSB.gov. Accessed June 11, 2018, https://www.ntsb.gov/about/reports/Documents/FY2018-2022strategicPlan.pdf.

National Transportation Safety Board. (n.d.). “ Information for Emergency Responders, Government Agencies, and Public Safety Personnel.” NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/tda/er/Pages/default.aspx

National Transportation Safety Board. (2016). “National Transportation Safety Board Fiscal Year 2017 Budget Request.” NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/about/reports/Documents/NTSB_FY2017_Budget.pdf

National Transportation Safety Board. (n.d.). “Safety Advocacy.” NTSB.gov. Accessed June 25, 2018 at https://www.ntsb.gov/safety/Pages/default.aspx

National Transportation Safety Board. "The Investigative Process." NTSB.gov. Accessed June 11, 2018, https://www.ntsb.gov/investigations/process/Pages/default.aspx.

NSF Cybersecurity Ideas Lab. (2014). “Interdisciplinary Pathways Towards a More Secure Internet.” February 10-12, https://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf

Obama, B. (2016). “Presidential Policy Directive — United States Cyber Incident Coordination.” White House: Office of the Press Secretary. Accessed June 25, 2018 at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Reuters. (2017). “U.S. blames North Korea for 'WannaCry' cyber attack.” Reuters.com. December 18, https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

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

Rosenzweig, P. (2018). “The NTSB as a Model for Cybersecurity.” R Street. May, https://2o9ub0417chl2lg6m43em6psi2i-wpengine.netdna-ssl.com/wp-content/uploads/2018/05/Final-Short-No.-58.pdf

Shackelford, S. (2018). “How Airplane Crash Investigations Can Improve Cybersecurity.” The Conversation. February 22, https://phys.org/news/2018-02-airplane-cybersecurity.html

Shackelford, S. & Brady, A. (2018). “Is it Time for a National Security Safety Board?” Albany Law Journal of Science and Technology, Kelley School of Business Research Paper No. 18-34. January 12, https://ssrn.com/abstract=3100962

US-CERT website. (n.d.). Accessed June 25, 2018 at https://www.us-cert.gov/

US-CERT. (n.d.). “HIDDEN COBRA - North Korean Malicious Cyber Activity.” us-cert.gov. Accessed June 25, 2018 at https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity

US-CERT. (n.d.). “Tips.” US-CERT.gov. Accessed June 25, 2018 at https://www.us-cert.gov/ncas/tips

USDA. (2018). “Medical Devices: Cybersecurity.” FDA.gov. April 17, https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

U.S. Government Accountability Office. (n.d.). “Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information - High Risk Issue.” GAO.gov. Accessed June 25, 2018 at https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary

Volz, D. (2018). “Tech firms, including Microsoft, Facebook, vow not to aid government cyber attacks.” Reuters.com. April 17, https://www.reuters.com/article/us-usa-cyber-microsoft/tech-firms-including-microsoft-facebook-vow-not-to-aid-government-cyber-attacks-idUSKBN1HO283

Wolfe, J. (2017). “Cyber attack could spark lawsuits but not against Microsoft.” Reuters.com. May 15, https://www.reuters.com/article/us-cyber-attack-liability/cyber-attack-could-spark-lawsuits-but-not-against-microsoft-idUSKCN18B2SE