2020 RESOURCES FOR MEASURING CYBERSECURITY

A PARTIAL ANNOTATED BIBLIOGRAPHY

Kathryn Waldron

R Street

TABLE OF CONTENTS

INTRODUCTION

Last year, the R Street Institute published a bibliography of cybersecurity resources.[1] This bibliography was part of a broader initiative to build a consensus around publicly agreed upon metrics to assess cybersecurity. As part of this initiative, our team met with various academics and industry stakeholders to discuss measurements and found that very little consensus existed around best practices, let alone whether it was possible to develop widely used metrics. The best practices that did exist—along with other innovative attempts to create cybersecurity metrics—were compiled and published by our team. As we are policy specialists and not information technology (IT) professionals, our goal in releasing the bibliography was not to exhaustively list every company or academic paper ever created, but to provide a survey of the different types of models and methodologies in use.

Our intention is to make the bibliography an annually updated, living document that evolves over time, as new research is published and as we develop a greater understanding of the field. Below you will find this year's additions to this compendium. We hope the resources listed below provide either further illumination to the methods previously described or introduce new initiatives worthy of consideration.

1 Kathryn Waldron, "**Resources for Measuring Cybersecurity: A Partial Annotated Bibliography**," R Street Institute, October 2019.

FRAMEWORKS

As mentioned in our previous bibliography, the most common method used to assess an organization's cybersecurity posture is also the simplest: adopt or create a list of standards and best practices—typically called a framework—and compare the security precautions implemented with those recommended. Although an organization can create their own best practices, many of the most popular frameworks are from government bodies or international standards-setting organizations. They vary from practices designed to be broadly adopted to those specifically tailored to a particular industry.

The benefit of frameworks is their straightforward nature. They are most valuable to organizations whose cyber hygiene is generally lacking, and to small- or medium-sized enterprises that have limited resources to devote to IT. If a company has failed to implement many industry best practices or is looking to determine a minimum baseline of risk mitigation, it is fairly safe to assume that adopting a framework would be beneficial, even if it is impossible to quantitatively determine just how beneficial.

However, frameworks are also problematic. Because they are intended to reach a broad audience, they may recommend practices that aren't relevant or ignore a company's particular needs. Many organizations also follow a framework in name, but struggle to implement the recommendations in practice. This can be due to a number of factors, including budget constraints, a limited number of IT professionals, lack of adequate workforce training or deprioritization at the executive level. Additionally, adopting a framework can instill a false sense of security in these situations, which can lead organization leaders to believe their cyber hygiene is better than it actually is.

In last year's bibliography we provided a list of some of the most common frameworks. However, many organizations may not know how these frameworks differ from one another or which framework is most appropriate for their organization. Below we have included some articles and reports that provide a broader context for why organizations pick the frameworks they do, and the challenges presented.

PICKING A FRAMEWORK

Olivia Giuca et al., "A Survey of Cybersecurity Risk Management Frameworks," *Soft Computing Applications* 1 (2018), pp. 240-272.

This paper discusses the key drivers that motivate an organization to adopt a cybersecurity framework and provides a survey of several of the most common frameworks and standards. The authors also identify criteria organizations can use when comparing frameworks in addition to their own evaluation of certain frameworks.

"Survey Report: Trends in Security Framework Adoption," Dimensional Research and Tenable Network Security, March 2016.

This report surveyed over 388 IT and security professionals regarding which security frameworks their company adopted, why the particular framework in question was chosen and how well the framework was implemented.

Frank Kim, "How to Make Sense of Cybersecurity Frameworks," RSA: RSA Conference, March 6, 2019.

Frank Kim teaches how to organize and distinguish between different types of frameworks, ways to use multiple frameworks and how to communicate the results.

THE EFFICACY OF FRAMEWORKS

"Trends in Cybersecurity Frameworks and Foundational Controls—a Survey of IT Security Professionals," Dimensional Research, Center for Internet Security and Tenable Network Security, January 2018.

This report—which analyzes survey data from 324 IT security decision makers at various companies—found that many companies struggled to appropriately adopt cybersecurity frameworks. Most companies faced constraints of some kind, such as budget issues or a lack of prioritization. Many companies used more than one framework but had not automated the security controls suggested.

"Cybersecurity Frameworks and Foundational Security Controls: A Survey of IT Security Professionals," Dimensional Research, Center for Internet Security and Tenable Network Security, November 2016.

This survey finds that while many organizations initially face challenges when adopting frameworks, they are more likely to be positive about their overall security program after having utilized a framework for 12 months or more.

CYBER INSURANCE

Last year we also highlighted the growing cyber insurance market and the various challenges cyber insurance companies face. Because cyber insurance is still a nascent industry, there is limited data available to accurately assess and price policies. In addition, many companies are hesitant to share information about their own cyber vulnerabilities. And while data may exist about certain common types of cyber incidents—such as ransomware or phishing—the cyber vulnerability landscape is constantly shifting as hackers develop new types of attacks. By focusing on previous threats, a cyber insurance policy may not offer accurate or appropriate coverage. Another difficulty is measuring the resultant cost of a successful cyberattack. While there may be a direct financial loss, the company may also be impacted by more intangible costs—such as losing future business due to a damaged reputation.

Listed below are several resources that provide a greater overview of the current cyber insurance market:

Office of the Chief Economist, "Assessment of the Cyber Insurance Market," U.S. Dept. of Homeland Security, July 2019.

This report provides an overview of the cyber insurance market. It finds the myriad difficulties of underwriting cyber insurance are "limiting the potential of the cyber insurance market and the pace at which the market is evolving."

Andrew Granato and Andy Polacek, "The Growth and Challenges of Cyber Insurance," *Chicago Fed Letter* No. 426, Federal Reserve Bank of Chicago, 2019.

This newsletter includes a brief history of cyber insurance and provides an overview of some challenges insurers have faced in determining how to underwrite and price cyber insurance policies. Problems identified and explored include: the limited loss history insurers can draw upon for information, the constant evolution of types of cyberattacks, the scale of damage caused when multiple companies fall victim to the same attack and the cascading nature of the damage.

Savino Dambra et al., "SoK: Cyber Insurance—Technical Challenges and a System Security Roadmap," Institute of Electrical and Electronics Engineers: 41st IEEE Symposium on Security and Privacy, May 20, 2020.

Dambra, Bilge and Balzarotti look at the academic research that has been conducted on cyber insurance, with particular focus on the economic aspects, the mathematical models, the risk management methodologies and the predictions of cyber events. They then propose several additional areas where further research would allow quantitative approaches to replace the current qualitative methods.

Gregory Falco et al., "A Research Agenda for Cyber Risk and Cyber Insurance," Harvard School of Engineering and Applied Sciences: Workshop on the Economics of Information Security, June 3, 2019.

Falco and his co-authors argue that "[I]ndustry and academic research on cyber risk in all its complexity has been piecemeal and uncoordinated." They look at the different contributions various fields of study have made toward researching cyber insurance and propose a model that identifies how to utilize and synthesize further cross-disciplinary research.

Sasha Romanosky et al., "Content analysis of cyber insurance policies: how do carriers price cyber risk?", *Journal of Cybersecurity* 5:1 (Feb. 27, 2019).

The authors accumulated over 100 cyber insurance policies filed with state insurance commissioners. They looked at differences in coverage, the types of questions insurers asked companies to assess their risk and the methods used to price policies.

Xiaoying Xie et al., "Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market," *The Geneva Papers on Risk and Insurance* 45 (2020), pp. 690-736.

Xie, Lee and Eling analyze the current U.S. cyber insurance market and find that insurers entering the space do so because they believe they have a competitive advantage in understanding and pricing cyber risks. They also find that the amount and type of coverage offered differs substantially across insurers.

CYBERHEDGE

In the past year, our team came across Cyberhedge, which is a company that uses a different market approach to measuring cybersecurity. Cyberhedge brands itself as the "first financial tool for instantly pricing cyber risk."[2] Instead of focusing on inside information to determine a company's cyber posture, Cyberhedge uses external information to build their Cyber Governance Indices.

Christopher Nolan et al., "Cybersecurity: today's most pressing governance issue," *Journal of Cyber Policy* 4:3 (2019), pp. 425-441.

The authors discuss cyber hygiene and add their own definition of Cyber Value at Risk, which they deem a "financial component of a benchmarking exercise necessary to determine cyber governance quality at an enterprise level."

2 "**What we do**," Cyberhedge, last accessed Oct. 5, 2020.

THE CYBERGREEN INSTITUTE

Another organization worthy of attention is the CyberGreen Institute, a non-profit that "serves the global public benefit by supporting a more resilient and healthier global Internet Ecosystem."[3] Their dedication to identifying and providing "evidence-driven metrics and measurements" has led to the development of the CyberGreen Statistics platform, which monitors several key risk indicators and compares the performance of the internet and vulnerability to denial-of-service attacks across the globe.[4]

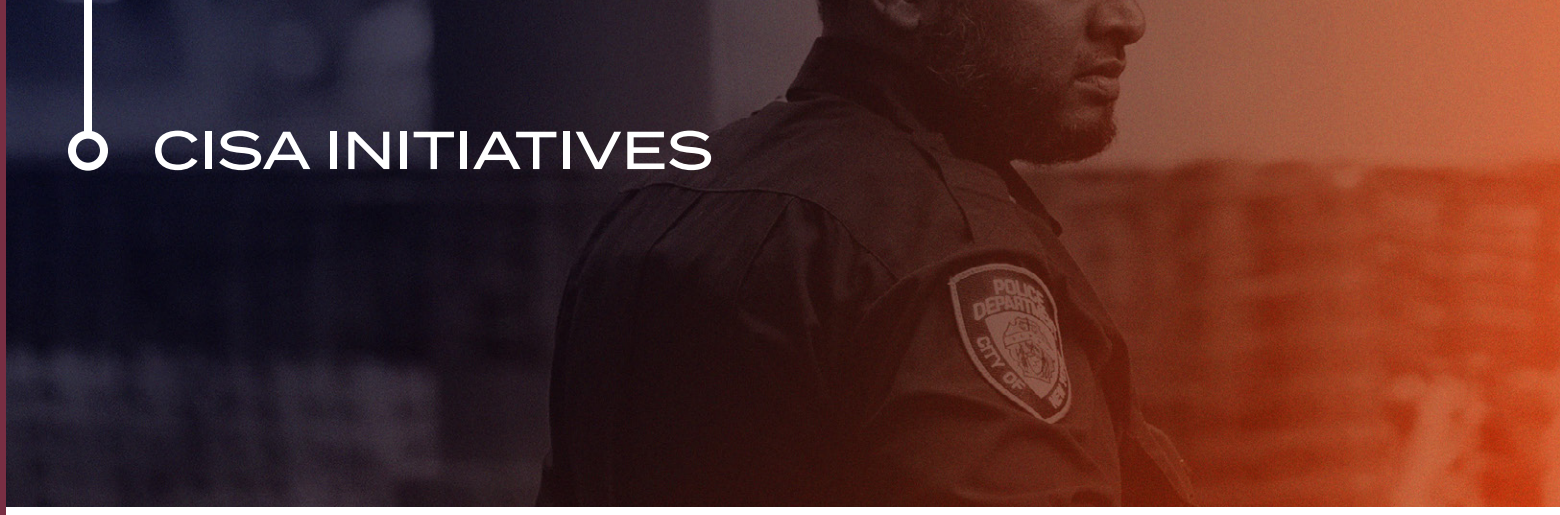
"The Cyber Green Initiative: Improving Health Through Measurement and Mitigation," Japan Computer Emergency Response Team Coordination Center, Aug. 10, 2014.

The organization's concept proposal, which lays out their purpose and history in greater detail.

"Cyber Green Research Paper," Japan Computer Emergency Response Team Coordination Center, Winter 2015.

This research paper looks at the lack of rigorous cybersecurity metrics, with a particular focus on cyber health. The report argues the reasons behind this omission are numerous, including issues in collection, the inability to cross-compare data and a failure to apply normalization techniques. This failure to develop appropriate metrics prevents organizations from effectively comparing and evaluating potential security solutions.

3 "Who We Are," CyberGreen, last accessed Oct. 5, 2020.
4 Ibid.



CISA INITIATIVES

In last year's bibliography we highlighted the Cyber Risk Economics (CYRIE) project run by the Department of Homeland Security's (DHS) Science and Technology Directorate.[5] However, CYRIE isn't the only project under the DHS. The DHS's Cybersecurity and Infrastructure Agency (CISA) has a variety of resources and projects that may also assist in measuring cybersecurity.

ASSESSMENT SERVICES AND TOOLS

CISA offers a range of services and assessment tools aimed at assisting the "Federal Government; State, Local, Tribal and Territorial Government; Private Industry; Academia; NGO and Non-Profit; and General Public stakeholders."[6] One such tool is the Cyber Security Evaluation Tool (CSET®), a desktop application designed to assist an organization with evaluating their own information security.[7] Other services include, but are not limited to: vulnerabilities scanning, phishing and cyber resilience assessments, and remote penetration testing. A complete list of services offered by CISA can be found in their catalog.[8]

MEASUREMENT BEST PRACTICES

CISA also offers a library of information security best practices which includes their own bibliography of literature on measuring cybersecurity. However, these documents do not appear to have been updated since 2013. [9]

NATIONAL CRITICAL FUNCTIONS SET

In April 2019, CISA's National Risk Management Center (NRMC) released the National Critical Functions (NCF) Set on CISA's work to manage the most strategic risks to our nation.[10] This is a one-page resource that lists the 55 National Critical Functions, described as: "The functions of government and the private sector [...] so vital that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[11]

5 Science and Technology Directorate, "**Cyber Risk Economics**," U.S. Dept. of Homeland Security, 2019.
6 Ibid.
7 Ibid.
8 Cybersecurity and Infrastructure Security Agency, "**Services Catalog**," U.S. Dept. of Homeland Security, Summer 2020.
9 Cybersecurity and Infrastructure Security Agency, "**Measurement**," U.S. Dept. of Homeland Security, last accessed Oct. 1, 2020.
10 National Risk Management Center, "**National Critical Functions Set**," Cybersecurity and Infrastructure Security Agency, last accessed Oct. 1, 2020.
11 Ibid.

NIST PROJECTS

The National Institute of Standards and Technology (NIST) has published two of the most common frameworks used for measuring cybersecurity: NIST 800-53—which set the cybersecurity standards for most federal agencies and government contractors—and the NIST Cybersecurity Framework (NIST CSF), which was created to be used more broadly.[12] However, NIST also has several other projects that focus on security metrics.

NIST MEASUREMENTS FOR INFORMATION SECURITY PROJECT

According to the NIST website, the project seeks to:

- Create a compilation of tools, research, standards and guidelines that address cybersecurity measurements.
- Participate actively in voluntary standards initiatives related to cybersecurity measurements.
- Develop a collaborative space for the community to share views and resources that relate to cybersecurity measurements.
- Develop a roadmap to address and advance cybersecurity measurement challenges and solutions.[13]

NIST CYBERSECURITY RISK ANALYTICS PROJECT

According to the NIST website, the goal of the Cybersecurity Risk Analytics (CRA) project is to "enable information sharing among risk owners about historical, current and future cyber risk conditions."[14] The project also intends "to help not only enhance existing cyber risk mitigation strategies but also improve and expand upon existing cybersecurity risk metrology efforts."[15] In addition, the CRA aims to create partnerships with individuals and organizations from both the public and private sectors to build a repository where members can share information regarding cyber breaches.

12 "SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Sept. 2020. ; "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, April 16, 2018.

13 "Measurements for Information Security," The National Institute of Standards and Technology, Sept. 24, 2020.

14 "Cybersecurity Risk Analytics," The National Institute of Standards and Technology, Sept. 10, 2020.

15 Ibid.

NIST ALGORITHMS FOR INTRUSION MEASUREMENT (AIM) PROJECT

"The Algorithms for Intrusion Measurement (AIM) project furthers measurement science in the area of algorithms used in the field of intrusion detection. The team focuses on both new detection metrics and measurements of scalability (more formally algorithmic complexity). This analysis is applied to different phases of the detection lifecycle to include pre-emptive vulnerability analysis, initial attack detection, alert impact, alert aggregation/correlation, and compact log storage. In performing this work, the AIM project seeks to enhance our nation's ability to defend itself from network-borne attacks."[16]

NIST NATIONAL VULNERABILITY DATABASE (NVD)

"The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics."[17]

16 **"Algorithms for Intrusion Measurement."** The National Institute of Standards and Technology, June 22, 2020.
17 "**National Vulnerability Database**," The National Institute of Standards and Technology, last accessed Oct. 1, 2020.

ACADEMIC EFFORTS

THE ECONOMICS OF CYBERSECURITY

Lawrence A. Gordon et al., "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *Journal of Cybersecurity* 6:1, 2020.

Gordon, Loeb and Zhou attempted to integrate the cost–benefit analytical approach of the Gordon-Loeb model with the NIST Cybersecurity Framework. Their analysis may help firms determine which tier of the NIST cybersecurity framework they should implement.

Rachel Rue and Shari Lawrence Pfleeger, "Making the Best Use of Cybersecurity Economic Models," IEEE Security & Privacy 7:4 (2009), pp. 52-60.

Rue and Pfleeger compared several economic models used to model cybersecurity. They determined that many models are based on the same unrealistic assumptions and made several suggestions for future improvements.

Rok Bojanc and Borka Jerman, "Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System," *Organizacija* 45:6 (November 2012).

Bojanc and Jerman propose their own quantitative model, which they suggest differs from other economic models of cybersecurity as it allows for direct comparison and quantitative assessment of different security measures.

Rok Bojanc and Borka Jerman-Blažič, "A Quantitative Model for Information-Security Risk Management," *Engineering Management Journal* 25:2 (2013), pp. 25-37.

Bojnac and Jerman-Blažič further develop their own economic model designed to systematically guide an organization in evaluating their security risk and choosing the appropriate security solutions. The authors then test their model with data from real businesses.

Paresh Rathod and T. Hämäläinen, "A Novel Model for Cybersecurity Economics and Analysis," Institute of Electrical and Electronics Engineers: 2017 IEEE International Conference on Computer and Information Technology, Aug. 23, 2017.

The authors propose a model based on their own Cybersecurity Readiness Level Metrics that will harmonize existing European cybersecurity initiatives.

CYBER RESILIENCE

Don Snyder et al., "Measuring Cybersecurity and Cyber Resiliency," RAND Corporation, 2020.

This report presents a framework for the development of two types of metrics designed to estimate the potential performance of a U.S. Air Force mission or system in a cyber-contested environment. The framework incorporates working-level metrics to counter an adversary's cyber operations and institutional-level metrics to capture any cyber-related organizational deficiencies. The authors then determine how to provide a score for missions or systems based on the framework.

Richard Kerkdijk, "Library of Cyber Resilience Metrics, Rabobank," ABN AMRO, ING Bank and TNO, 2017.

This collaborative report is a collection of 47 metrics used to determine cyber resilience.

Deborah Bodeau and Richard Graubart, "Cyber Resilience Metrics: Key Observations," The MITRE Corporation, 2016.

This paper evaluates many of the metrics used to measure cyber resilience and argues that no single cyber resiliency metric or set of metrics will work for all environments.

Deborah Bodeau et al., *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods,* The MITRE Corporation, September 2018.

Bodeau and her fellow authors provide a general reference of cyber resilience metrics for systems engineers, program management staff and others concerned with assessing or scoring cyber resiliency for systems and missions. They address how scoring, metrics and measures of effectiveness (MOEs) can be used by systems engineers and program managers to identify potential areas for improvement and to evaluate the potential benefits of alternative solutions.

Alexander Kott et al., "Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153," U.S. Army Research Laboratory, April 2018.

Kott and his fellow authors discuss measuring cyber resilience specifically within the context of military operations, using either a metrics-based or model-based approach. They argue that resilience is inherently a time-based problem and that current models lack the necessary focus on a granular data.

CONFERENCES

Presentations related to cybersecurity metrics and measurement can be found at nearly all conferences related to IT or information security, as well as many others. Listed below are some of the relevant conferences. The chosen conferences were included either due to prominence or a more limited focus on metrics.

Metricon

Workshop on the Economics of Information Security

IEEE

International Workshop on Traffic Measurements for Cybersecurity

RSA

Security Metric Summit

Finally, here are some of the most consequential works published by R Street scholars that focus on measuring cybersecurity:

Paul Rosenzweig, "**Progress in Cybersecurity: Toward a System of Measurement**," ***Lawfare***, May 24, 2019.

Rosenzweig argues that any useful measurement system must be objective; capable of being quantified; commensurate and intercomparable across different cybersecurity approaches and systems; usable for decision-makers in allocating limited resources; and widely agreed upon and generally accepted within the relevant communities. He identifies two new contributions to the field: the BSA framework and CISA's national critical functions set, both of which are included in greater detail in this bibliography.

Paul Rosenzweig, "Preliminary Observations on the Utility of Measuring Cybersecurity," *Lawfare*, Aug. 6, 2019.

Rosenzweig summarizes his conversations with other thought leaders and industry specialists regarding cybersecurity metrics. He groups their responses into three categories: those who believe their respective organization already adequately measures cybersecurity, those who believe it is futile to attempt to quantitatively measure an organization's cybersecurity in any holistic or meaningful manner and those who wish for better systems of measurement but lack the knowledge to create one. He then discusses the merits and shortcomings of each position.

Paul Rosenzweig, "The NDAA Pushes Forward on Cyber Metrics," *Lawfare*, Jan. 2, 2020.

Rosenzweig discusses section 800 of the 2020 National Defense Authorization Act, which requires the Department of Defense to provide:

> *assurances that cybersecurity metrics of the software to be acquired or developed, such as metrics relating to the density of vulnerabilities within the code of such software, the time from vulnerability identification to patch availability, the existence of common weaknesses within such code, and other cybersecurity metrics based on widely-recognized standards and industry best practices, are generated and made available to the Department of Defense and the congressional defense committees.*

Paul Rosenzweig, "Assessing Cyber Risk From External Information," *Lawfare*, May 11, 2020.

Rosenzweig debates the possibility of assessing an organization's cyber risk based on publicly available information, instead of internal audits. He points out that internal information is often difficult to acquire and that assessing the potential loss from other types of risk is often done based on external information in markets.

Kathryn Waldron, "Resources for Measuring Cybersecurity: A Partial Annotated Bibliography," R Street Institute, Oct. 2019.

The previous iteration of this bibliography.

CONCLUSION

Without a universal system of measurement to evaluate cybersecurity, many companies and organizations lack the ability to appropriately assess their own security. And without the ability to discern best practices, organizations constrained by limited security budgets—such as local and state governments and smaller businesses—will remain especially vulnerable to underinvestment in cybersecurity. As long as the financial costs of implementation are known and the expected benefits remain unknown, cybersecurity investments will never accurately match up with the risk landscape.

As our team pursues superior methods of measuring cybersecurity, we plan to update and publish worthy additions to this bibliography on an annual basis.

ABOUT R STREET

The R Street Institute is a nonprofit, nonpartisan, public-policy research organization ("think tank"). Our mission is to engage in policy research and outreach to promote free markets and limited, effective government. In addition to our D.C. headquarters, we have offices in Georgia, Texas, Ohio, Massachusetts and California, covering the Southeast, Central, Midwest, Northeast and Western regions, respectively.

We work extensively on both state and national policy, focusing on issues that other groups tend to neglect. Our specialty is tackling issues that are complex, but do not necessarily grab major headlines. These are the areas where we think we can have a real impact. We believe free markets work better than the alternatives. At the same time, we recognize the legislative process calls out for practical responses to current problems. Toward that end, our motto is "Free markets. Real solutions."

INDEPENDENCE STATEMENT

The R Street Institute is committed to producing high-quality research and educating federal, state and local policymakers. Facts, data and staff expertise drive our research. We do not and will not permit the interests of politicians, donors or any other third party to dictate R Street's research or policy positions. While R Street may solicit input from any number of interested stakeholders, we are solely responsible for our research and related activities. Even where we agree with stakeholders and donors, R Street staff does not and will not represent, lobby or advocate on behalf of any third party.

Kathryn Waldron is a fellow at the R Street Institute, where she researches and writes on cybersecurity and other national security policy issues.

R STREET INSTITUTE
1212 New York Avenue, NW, Suite 900
Washington, D.C. 20005
(202) 525-5717 feedback@rstreet.org
www.rstreet.org