Atlantic Council

BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

BREAKING THE CYBER-SHARING LOGJAM

by Jason Healey

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005

ISBN: 978-1-61977-970-9
Publication design: Krystal Ferguson

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council, its partners, and funders do not determine, nor do they necessarily endorse or advocate for, any of this report's particular conclusions.

February 2015

TABLE OF CONTENTS

CYBER STATECRAFT INITIATIVE

The focus of the Cyber Statecraft Initiative is to examine the overlap of traditional national security, international relations, and economic security with the emerging challenges and opportunities of cyberspace.

The Cyber Statecraft Initiative has accordingly made its mission "Saving Cyberspace." The initiative's many novel ideas and projects help realize this vision in Washington and other national capitals and technology centers.

The initiative helps Fortune 500 companies, governments, and other stakeholders to position themselves as thought leaders in cyber statecraft—the key tool in generating innovative solutions for a better Internet.

BREAKING THE CYBER-SHARING LOGJAM

Introduction

The Internet makes everyone neighbors in cyberspace, connected by a digital infrastructure that serves as the bedrock of their communities. But the neighborhood watch system is broken. The information sharing between well-intentioned residents of cyberspace is insufficient for defending against the myriad cyber threats that confront state and nonstate actors alike.

Despite pockets of excellence, states and nonstates have not been able to effectively share information about cyber incidents and vulnerabilities. Cost structures and risks are often too high to justify the investment and time required for information sharing, especially when no one seems sure how to accurately measure its gains. Sharing also depends on trust, which takes time to develop and is hard to scale.

There is good reason to push for more robust collaboration. Cyber sharing can have a powerful impact on stopping malicious attacks, and can quickly identify and fix systemic vulnerabilities.

The most active cyber-sharing organizations usually find that collaboration is worth the investment of time and effort, as it significantly improves their cyber defenses. The issue is how to get organizations deep enough into the sharing process that the rewards outweigh the risks.

Sharing is the focus of many conferences, speeches, and legislative bills. But while the act of cyber sharing is critical, it is not the entire story. Information sharing threatens to become an end in itself, rather than a means to the end of actually closing vulnerabilities, stopping espionage operations, and defeating denial-of-service (DoS) attacks. A more balanced approach will work to break the sharing logjam, with an eye toward these more fundamental cybersecurity outcomes.

To make this case, this report analyzes best practices in the area of cyber sharing, describes various axes of sharing and the objectives of each, and provides recommendations for goal-directed information sharing.

NOT ALL KINDS OF SHARING ARE EQUAL, AS MANY ORGANIZATIONS INVOLVED IN CYBER DEFENSE ARE NET CONSUMERS—NOT SUPPLIERS—OF SHAREABLE CYBERSECURITY INFORMATION.

Understanding Sharing

It has been more than fifteen years since cyber information sharing was first a government priority, featuring heavily in US President Bill Clinton's Presidential Decision Directive 63 (PDD 63). That document created US government organizations to facilitate sharing and called on the nonstate critical infrastructure sectors to create Information Sharing and Analysis Centers (ISACs). Some of these ISACs have been effective (see box 1) but after a decade and a half, sharing has still fallen short of what the President intended.[1]

Aware of the benefits of enhanced information sharing, the Barack Obama administration now hopes to bolster cooperation across five axes:

USG↔USG: Sharing within the US federal government, such as between the Department of Homeland Security (DHS), the Department of Defense (DoD), the Department of Justice (DoJ), and the Federal Bureau of Investigation (FBI).

USG↔S&L: Sharing between federal government agencies and state, local, and tribal governments (and, to a lesser degree, between those entities directly).

USG↔FG: Sharing internationally between the federal government and foreign governments.

1 White House, Presidential Decision Directive 63: Critical Infrastructure Protection, May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

USG↔PS: Sharing between the federal government and the private sector.

PS↔PS: Sharing between companies and nonstate actors, all within the private sector.

BOX 1. PDD 63 ON INFORMATION SHARING AND ANALYSIS CENTERS (1998)

The [US government] shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the [US government and the White House] shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing, and disseminating private sector information to both industry and the [US government]. The center could also gather, analyze, and disseminate information from the [US government] for further distribution to the private sector.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly in extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and nonregulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government.

While all forms of sharing are important, this classification system does not reflect significant differences between the axes. Not all axes are created equal.

For example, the sharing from government to the private sector can differ greatly from the reverse flow, from the private sector to government, as the information is used for very different purposes on either end of the spectrum. While the private sector usually wants very tactical and actionable information on threats, the government tends to prioritize determining which nations might be behind an attack, or gleaning general information to guide policymaking.

Moreover, many organizations involved in cyber defense are net consumers of shareable cybersecurity information, rather than suppliers. For example, state and local governments must fix their own cyber problems, and only rarely possess significant cybersecurity information not held elsewhere in the system.

The private sector is critical to solving any cybersecurity problem. Unfortunately, governments often treat it as monolithic: i.e., "the private sector needs to share more."

In reality, the private sector is highly differentiated. Most companies are predominantly consumers of information, ingesting what they need to better protect themselves. By comparison, the major software vendors, telecommunication providers, Internet service providers, and cybersecurity companies serve truly critical roles, because they have both a heavy demand for and a large supply of shareable information.

A recent report by a White House advisory group, comprising executives from telecommunications and information technology firms, addressed these issues. It split out the technology segment of the private sector to explore the critical but distinctive role each has to play in defeating cyberattacks. Companies producing software and devices, for instance, must develop and push security patches, while companies controlling network access (ICT enablers) and the core Internet can block or prioritize traffic, having potentially adverse consequences on the whole ecosystem.[2]

Of course, in order to enact such solutions, each type of company contributes different sets of sharable information.

The axes are a handy way to frame different sharing issues. But actual solutions are often more effective when tied to outcomes that fix the underlying problems the sharing is meant to address, as shown in table 1.

Challenges to Sharing

If the benefits of robust cyber sharing are readily apparent, why is the current quality of collaboration so inconsistent?

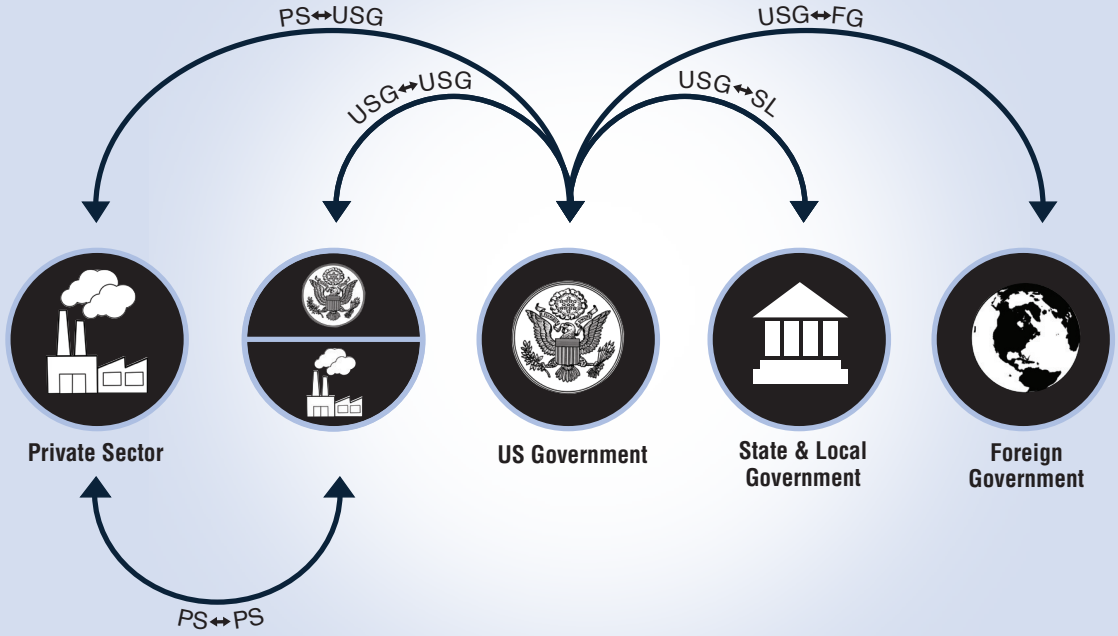
Put simply, the costs and risks of sharing currently outweigh the perceived value of a widespread information partnership. The status quo incentive structure encourages both firms and states to keep information close to the vest. In the private sector, information-security professionals are ever wary of backlash from customers or regulators, while governments keep too much information classified, or otherwise restricted from sharing. This is particularly true in the law enforcement and national security communities.

2 National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Information and Communications Technology Mobilization,* (draft and undated), http://www.dhs.gov/sites/default/files/publications/ICTM%20Final%20Draft%20Report%2011-2014%20%282%29.pdf.

TABLE 1.

Cyber Information Sharing

Aware of the benefits of enriched information sharing, the US administration hopes to bolster cooperation across five axes.



Cybersecurity Problem	Description	Axes Involved	ICT Companies Involved
Distributed Denial-of-Service (DDoS)	Fast-moving operations, mostly involving sharing between telecommunications firms, Internet service providers, and associated groups to defeat DDoS attacks. The more massive these attacks are, the more easily they are noticed.	**PS↔PS**	Access, Core, IP Services, Application/Content
Counter-Advanced Persistent Threat (APT)	Often-secretive government and corporate operations to spot and defeat sophisticated foreign espionage. Detecting and stopping such attacks is usually achieved by sharing the signatures of the specific attacks or indicators of when an organization has been compromised.	**USG↔USG** **USG↔PS** **PS↔PS**	User/Device, Customer Edge, Application/Content
Anti-Malware	During crises, a fast-moving response against outbreaks of malicious software, involving major software producers, security companies, sometimes the government, and even the backbone Internet community. Can also be less acute and more chronic, dealing with the slow and steady flow of new malware.	**PS↔PS** **USG↔USG** **USG↔PS**	User/Device, Customer Device, Application/Content
Botnet Takedown	Cooperative efforts between software and security companies, telecommunications firms, Internet service providers, and the government to tackle malicious networks of infected computers.	**PS↔PS** **USG↔USG** **USG↔PS** **USG↔FG**	User/Device, Core, IP Services
Major Vulnerability Response	Discovery of new computer vulnerabilities, passing that information to the creator of the software so that it can be fixed, creating patches and monitoring signatures, and pushing solutions to the community using that software.	**PS↔PS** **USG↔PS**	User/Device, Customer Edge

The five axes of sharing: USG↔USG (within the US government),**USG↔SL** (US federal government to state and local governments and vice versa),**USG↔FG** (US federal government to foreign governments and vice versa),**USG↔PS** (US federal government to private sector and vice versa), and **PS↔PS** (within the private sector). According to the NSTAC, the **six ICT enablers** are companies involved with users and devices, customer edge, access to the network, core network, Internet protocol services, and application and content.

When sharing does happen, it often occurs between individual practitioners who have established personal trust relationships through repeated interactions. But building trust this way lacks scalability. The on-ramps to developing trust are long, and there are too many off-ramps along the way that hinder the process. Without visible signs of trust and commitment from viable partners, other potential actors are often discouraged from joining the sharing community.

High transaction costs further constrain cyber sharing. The technology needed to build a platform for automated sharing, or to standardize information storage and exchange between partners, does not come cheap. Legal and regulatory risks abound, and bureaucratic inertia—in both the public and private sectors—adds additional friction to the process.

Information sharing is essentially one of the last great barter economies, often passed between friends and colleagues. A proper market for sharable information might unlock its true value and reward those who have the best leads. Money would chase value, helping to build scale.

Because sharing is currently considered an end in itself, most sharing metrics deal with process, rather than outcomes—asking how much was shared, instead of what was gained by sharing that information. Without effective metrics, the quality and relevance of shared information will remain uneven.

Governments are often perceived as wanting to be part of all solutions. But corporations are quick to point out that the US government's own internal sharing is limited, often for the same reasons that plague private firms.

Finally, even as governments note that the Internet is inherently global, most of their information-sharing schemes are stubbornly domestic, passing information back and forth with companies inside their own borders.

Examples of Successful Sharing

Sharing is elusive, but not impossible. There are many examples in which sharing works more or less smoothly.

One of the few truly successful examples of government sharing is the result of Executive Order 13636. Anytime the US government discovers that an American company had been victim, the new "default" is for the DHS or the FBI to notify that company with sufficient details to identify the attack.

For the past two years, the United Kingdom has run the Cyber-security Information Sharing Partnership (CiSP). Instead of limiting sharing to within a specific sector (such as retail or finance), the CiSP is one large, government-run sharing network, and it's having apparent initial success.[3]

3 CERT-UK, "Cyber-Security Information Sharing Partnership (CiSP)," https://www.cert.gov.uk/cisp/.

Most successful sharing networks, however, are not run by governments. The best-known examples of successful sharing are still those Information Sharing and Analysis Centers (ISACs) created in the United States in response to President Bill Clinton's request in 1998. Due to its strong operational responses in the face of attacks, the Financial Services ISAC (FS-ISAC) is widely considered to be the most effective. Its success is due, in part, to extremely deep-seated trust between participants, close cooperation with its government partners, and the continuous commitment of bank executives for more than fifteen years.

BECAUSE OF SUCCESSFUL SHARING IN THE FINANCE SECTOR, A TARGETED BANK MIGHT HAVE A BAD FIRST DAY, BUT WAS UNLIKELY TO HAVE A BAD SECOND DAY.

During a months-long campaign of denial-of-service attacks against the US financial sector (attributed by US officials to Iran) in 2012, whenever a new bank was targeted, it was likely to be quickly overwhelmed. But after the initial wave of attacks, fellow banks in the FS-ISAC—even though they might be competitors—came forward with the recipe to defeat the attacks. So even though a bank might have a bad first day, it was unlikely to have a bad second day.[4]

The FS-ISAC's success is built on extremely deep-seated trust between participants, close cooperation with its government partners, and the commitment of bank executives for more than fifteen years. Recently, the group has been active in sharing its lessons with the ISACs of other sectors and in enrolling non-US financial institutions in the program.

The Industry Consortium for Advancement of Security on the Internet (ICASI) is a coalition of major Internet companies intent on defeating cyberattacks by using multi-vendor approaches. Sharing works here, not just because the ICASI is a relatively tight-knit group—which makes trust easier—but because it is focused on outcomes. ICASI's secure collaboration portal is not the group's main activity; it is merely a supporting function to stop attacks, as exemplified by the group's Unified Security Incident Response Plan.[5]

A different kind of sharing has been pioneered by one of the major telecommunications companies with the Verizon Data Breach Investigations Report. Originally, this was a publication that broke ground in 2008 with detailed statistics on the five hundred intrusions which Verizon had investigated on

4 Conversation between the author and FS-ISAC executives, 2012.

5 Industry Consortium for Advancement of Security on the Internet, "The Unified Security Incident Response Plan," http://www.icasi.org/projects#usirp.

behalf of its clients. But unlike other similar reports, Verizon was able to attract other organizations, both public and private, to add their own data sources to give perhaps the best single source of such data with over sixty thousand incidents. And it is all because of sharing.

The final, and possibly most effective, sharing examples involve small, private groups. There are about two dozen tight trust networks of the most technically skilled defenders, all eager to collaborate with one another in order to thwart attacks. To join one of these groups, one "must be able to get your hands on a lever or a knob."[6] After all, "why share with organizations not in a position to deal with" the problem?

One such group is the Domain Name System Operations, Analysis, and Research Center (DNS-OARC), whose members are able to look at the data and make direct changes to the DNS system critical to keeping the Internet operating.[7]

Another of these relatively small but effective groups is NSP-SEC, which comprises the security experts of major network service providers (NSPs). This group "coordinates the interaction between [service providers] in near real time and tracks exploits and compromised systems as well as mitigates the effects of those exploits."[8] Like DNS-OARC and ICASI, it focuses on the outcome of stopping attacks, rather than on sharing. To maintain strong trust, participants must belong to a company that owns significant network resources. Participants must also be vouched for by at least two existing members.

This group was one of the few to make a difference against the massive denial-of-service attacks carried out against Estonia in 2007. One of the NSP-SEC representatives sent to help in Estonia expressed the group's role: "If something needs to be taken down, it needs to be taken down, and there isn't time for argument…that's understood up front [within NSP-SEC]…You can argue about it later."[9]

Current US Push

As of early 2015, new sharing projects have been launched in the United States. This is due to renewed energy for an information-sharing bill in Congress and a White House that has drafted a legislative proposal (and other projects) for information sharing.

The 115th Congress has taken up information sharing in its very earliest days, continuing the momentum from its predecessors. In January 2015, Representative Dutch Ruppersberger of the House Intelligence Committee reintroduced the exact same Cyber Intelligence Sharing and Protection Act (CISPA) sharing bill that passed the House in 2014.[10] The bill stalled in the Senate—in part from concerns over privacy—but generated wide support from technology companies like Facebook and Microsoft and industry associations such as the US Chamber of Commerce and Tech America.[11]

In its own legislative proposal, the White House seeks to create more sharing within the private sector (PS↔PS) in an effort to reduce the trust on-ramp and to extend the current model of the ISACs.

The proposal calls for the US government to "select a private entity to identify…a common set of best practices for the creation and operation of private information sharing and analysis organizations," or ISAOs.[12]

This set of best practices is meant to reduce obstacles so companies can join trust networks and begin sharing. One such practice is having clear "traffic light" protocols to indicate what information can be shared with whom, and under what conditions.[13] These new ISAOs are meant to be more flexible than the existing ISACs. Whereas ISACs are almost entirely based on national critical-infrastructure sectors, the new ISAOs can be organized in other ways—such as by locality or even internationally—as long as they meet the best practices.

Under this proposal, provided that Congress passes supporting legislation, a company will enjoy limited liability protection if it shares cyber threat information, either with an ISAO or with the Department of Homeland Security (DHS). DHS "will then share it in as close to real-time as practicable with relevant federal agencies and with private sector-developed and operated" ISAOs.[14]

6 Comment from Jeff Moss, founder of the DEF CON and Black Hat conferences (and an Atlantic Council Nonresident Senior Fellow), at Atlantic Council workshop on sharing, December 2014.
7 Domain Name System Operations Analysis, "Introduction to DNS-OARC," https://www.dns-oarc.net/.
8 NSP-SEC, "About NSP-Security," https://puck.nether.net/mailman/listinfo/nsp-security.
9 Bill Woodcock, "Building a Secure Cyber Future: Attacks on Estonia, Five Years On," transcript of the event hosted by the Atlantic Council in Washington, DC, May 23, 2012.
10 Cory Bennett, "House Dem Revives Major Cyber Bill," *Hill*, January 8, 2015, http://thehill.com/policy/cybersecurity/228945-top-house-dem-to-reintroduce-major-cyber-bill.
11 Hayley Tsukayama, "CISPA: Who's For It, Who's Against It," *Washington Post*, April 27, 2012, http://www.washingtonpost.com/business/technology/cispa-whos-for-it-whos-against-it-and-how-it-could-affect-you/2012/04/27/gIQA5ur0lT_story.html.
12 United States Office of Management and Budget, "White House Legislative Proposal on Cybersecurity Information Sharing," http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf.
13 For example, "red" information cannot be shared with anyone outside a subgroup, while "green" information may be shared with all members and government; Financial Services Information Sharing & Analysis Center, "Operating Rules," http://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2012.pdf.
14 White House, "Securing Cyberspace," http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

Recommendations for Increased Cyber Sharing

Practical solutions can increase the positive value and trust of sharing—enabling and encouraging future collaboration—and can reduce the associated expense and risk. The best alternatives will be built to achieve both of these goals.

In order to ratchet up the value and trust of sharing while limiting the costs and risks, policymakers and practitioners in both the private and public spheres should concentrate their efforts on three key areas.

First, the United States is focused on reducing the transaction costs of cyber sharing, to subsequently shorten on-ramps for building trust. It should continue these efforts, and should add common-sense extensions to its current policy push, from which other nations can draw lessons.

The Obama administration's goal is to encourage sharing within the private sector, but this might require more than just encouragement and standards. The government should put money where its policy is with a grant process to direct funds to nonstate groups already involved in effective cyber sharing. The government should also encourage major companies to match grants through their charitable foundations, or to initiate similar efforts of their own. Many nonstate sharing groups avoid publicity and interaction with national governments, but many could benefit from such cooperation—particularly if the economic incentives of interaction are improved.

To encourage sharing across national borders, the United States should invite comments from foreign partners as it develops its standards for ISAOs. Once the program is in place, the US government and foreign governments alike must encourage new ISAOs that are inherently international.

Governments should also become peer participants in nonstate information-sharing networks. Many governments, particularly in the United States, have massive networks and own key Internet infrastructure. Yet, they do not actively participate in nonstate groups that share information to keep the Internet operating smoothly, such as DNS root operator networks.

Governments should create sharing ombudsman positions in departments with sharable critical intelligence to ensure information is quickly declassified and shared. Within the United States, such positions could be established at the DHS, the FBI, the Office of the Director of National Intelligence (DNI), and the National Security Agency (NSA) and Central Intelligence Agency (CIA).

Second, nations must shift from sharing information as an end in itself to a broader focus on goals and outcomes. There are several ways to make this shift: articulate a clear vision and goals, develop incident-response plans, and encourage problem solving.

Governments need clear goals for sharing. Too often they have confusing sharing policies, which are split between the sometimes conflicting goals of stopping attacks or attributing them to specific nations or actors. To make the greatest difference, governments should deemphasize attribution and focus instead on halting the actual attacks.

Nations and organizations must drive their information-sharing efforts with crisp, well-thought-out incident response plans. After all, how can organizations know what information needs to be shared if they don't know how to respond to different kinds of incidents? Does the needed information have to be shared at all, or could it instead be discovered or simply purchased?

Plans should identify who is responsible for the decisions to stop the major classes of attacks—DDoS, counter-APT, anti-malware, botnet takedown, and major vulnerability response—and then work backwards from those outcomes to determine the information requirements needed to effectively take those actions.

In the United States, the process to develop a National Cyber Incident Response Plan has stalled, stuck in debates about bureaucratic roles and responsibilities. In such cases, nations can also look backward, starting with case studies of past incidents to develop initial response plans and information requirements. These case studies should then inform future response plans.

Within the United States, DHS should fund the Homeland Security Studies and Analysis Institute (or a similar academic center or think tank) to create case studies of major past incidents of various types—e.g., Conficker, botnet takedown. This center should map the actors, actions, and decisions involved in each case, as well as the necessary information and the sources of that information.

Nearly all of the most successful sharing groups share information only incidentally; their core mission is stopping cyberattacks or closing vulnerabilities. So government policy should be equally focused on encouraging groups that solve problems, rather than just sharing information. For example, in the United States, the new ISAOs that the White House is pushing are a good idea—but they will likely be far more successful if they primarily respond to incidents.

The recent report to the White House, mentioned above, on how technology companies can mobilize to respond to major incidents is an excellent foundation on which to build. It proposes structures and processes to tackle the truly strategic cyberattacks and failures; the sharing of information to win those battles is treated as a supporting function. Accordingly, the White House and other national governments should work with the technology sector to implement the recommendations from the report.

Sometimes, the best solution is to approach a problem sideways instead of head on. With cybersecurity, defenders should identify ways to get information besides sharing it. Actionable information is already pooling throughout

cyberspace, waiting to be collected and analyzed. For example, as noted in a past Atlantic Council issue brief on NATO, most of the defense information that NATO needs is in the hands of cybersecurity companies.[15] In situations like this, a focus on sharing is not the best mindset, as "getting threat data from cybersecurity companies does not require international agreements or trust relationships, just a credit card number."[16]

CYBERSECURITY INFORMATION IS LIKELY NO DIFFERENT THAN OTHER HUMAN ENDEAVORS WHERE MARKETS ARE THE MOST EFFICIENT WAY TO CLOSE A PERSISTENT MISMATCH BETWEEN THE DEMAND AND SUPPLY.

Third, governments and nonstate actors should explore how to unleash market forces. Currently, sharing is essentially a barter system, neither institutionalized nor part of a transparent marketplace. Cybersecurity information is likely no different than other human endeavors where markets can be an effective mechanism to close persistent mismatches between demand and supply.

One way to do this is for nations to encourage the creation of nonstate clearinghouses for specific needs. For example, a clearinghouse for attack signatures or indicators of compromise could assemble this information from the leading cybersecurity companies (or other companies with a massive global presence, such as tier 1 telecommunications providers) and combine it with similar information from intelligence agencies—thereby washing the original source, and creating an unparalleled global database. Any organization that contributes its signature collection would then be able to use the full database, while others could pay a fee to support the clearinghouse. Not only would critical infrastructure companies get an increased level of protection, so would the rest of the world's Internet users.

The aforementioned Homeland Security Studies and Analysis Institute would also be helpful in this endeavor.

Conclusion

Cyber sharing is hard. Too much information remains classified. The economic incentives are misaligned and the risks are high in what many organizations perceive as uncharted territory. But the benefits of sharing information can be significant. Organizations can learn valuable insights about their adversaries, the types of systems and information being targeted, the techniques used to gain access, and indicators of compromise.

Continuing to add more examples of successful collaboration will help build momentum for future sharing. It will take time to shift from a system of informal and semi-structured networks and relationships to a formal, institutionalized approach. Deepening the well of trust will be critical, and increasing the value of sharing will interest investors and policymakers alike.

Recognizing the value of collaboration, cybercriminals work in teams to exploit vulnerabilities in critical cyber infrastructure. Governments and companies should take a page from their adversaries' playbook. By working in tandem, the public and private sectors can bolster their defenses, reduce the efficacy of malicious attacks, and make cyberspace a more peaceful neighborhood for all.

15 Jason Healey and Leendert von Bochoven, "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO," Atlantic Council, 2012, http://www.atlanticcouncil.org/publications/issue-briefs/strategic-cyber-early-warning-a-phased-adaptive-approach-for-nato.

16 Ibid.

Atlantic Council

Board of Directors

CHAIRMAN
*Jon M. Huntsman, Jr.

CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

VICE CHAIRS
*Robert J. Abernethy
*Richard Edelman
*C. Boyden Gray
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson
*John Studzinski

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stephane Abrial
Odeh Aburdene
Peter Ackerman
Timothy D. Adams
John Allen
Michael Ansari
Richard L. Armitage
*Adrienne Arsht
David D. Aufhauser
Elizabeth F. Bagley
Peter Bass
*Rafic Bizri
*Thomas L. Blair
Francis Bouchard
Myron Brilliant
*R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Ashton B. Carter
James E. Cartwright
John E. Chapoton
Ahmed Charai
Sandra Charles
George Chopivsky
Wesley K. Clark
David W. Craig
*Ralph D. Crosby, Jr.
Nelson Cunningham
Ivo H. Daalder
Gregory R. Dahlberg
*Paula J. Dobriansky
Christopher J. Dodd
Conrado Dornier
Patrick J. Durkin
Thomas J. Edelman
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
Julie Finley
Lawrence P. Fisher, II
Alan H. Fleischmann
Michèle Flournoy
*Ronald M. Freeman
Laurie Fulton
*Robert S. Gelbard
*Sherri W. Goodman
*Stephen J. Hadley
Mikael Hagström
Ian Hague
John D. Harris II
Frank Haun
Michael V. Hayden
Annette Heuser
Jonas Hjelm
Karl Hopkins
Robert Hormats
*Mary L. Howell
Robert E. Hunter
Wolfgang Ischinger
Reuben Jeffery, III
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Lawrence S. Kanarek
Stephen R. Kappes
Maria Pica Karp
Francis J. Kelly, Jr.
Zalmay M. Khalilzad
Robert M. Kimmitt
Henry A. Kissinger
Peter Kovarcik
Franklin D. Kramer
Philip Lader
*Jan M. Lodal
*George Lund
Jane Holl Lute
William J. Lynn
*John D. Macomber
Izzat Majeed
Wendy W. Makins
Mian M. Mansha
William E. Mayer
Allan McArtor
Eric D.K. Melby
Franklin C. Miller
James N. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Obie L. Moore
*George E. Moose
Georgette Mosbacher
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Sean O'Keefe
Hilda Ochoa-Brillembourg
Ahmet Oren
*Ana Palacio
Carlos Pascual
Thomas R. Pickering
Daniel B. Poneman
Daniel M. Price
*Andrew Prozes
Arnold L. Punaro
*Kirk A. Radke
Teresa M. Ressel
Charles O. Rossotti
Stanley O. Roth
Robert Rowland
Harry Sachinis
William O. Schmieder
John P. Schmitz
Brent Scowcroft
Alan J. Spence
James Stavridis
Richard J.A. Steele
*Paula Stern
Robert J. Stevens
John S. Tanner
Peter J. Tanous
*Ellen O. Tauscher
Karen Tramontano
Clyde C. Tuggle
Paul Twomey
Melanne Verveer
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael F. Walsh
Mark R. Warner
David A. Wilson
Maciej Witucki
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
George P. Shultz
John W. Warner
William H. Webster

**Executive Committee Members*

List as of February 10, 2015

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org