THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

ADDRESSING SYSTEMIC CYBERSECURITY RISK

APPLIED RESEARCH PROGRAM

RESEARCH FELLOWS

Conor Cunningham
Cynthia Hannon
Mariam Malik
Rachel Paik
Rishi Paramesh
Heidi Samford
Kunat Sangcharoenvanakul
Sarah Sanguinet
Alison Wattles

SENIOR RESEARCH FELLOW

Alexander Wirth

PROGRAM MANAGER

Allison Anderson

FACULTY LEAD

Jessica Beyer

This report is a product of the Applied Research Program in the Henry M. Jackson School of International Studies at the University of Washington. The Applied Research Program matches teams of top-achieving Jackson School students with private and public sector organizations seeking dynamic, impactful, and internationally-minded analyses to support their strategic and operational objectives.

For more information about the Applied Research Program please contact us at jsisarp@uw.edu or visit our website at http://jsis.uw.edu/arp/

Addressing Systemic Cybersecurity Risk

Applied Research Program, Jackson School of International Studies

May 2018

Synopsis
Using financial systemic risk as an analogy for a hypothetical systemic cybersecurity risk regime, this report addresses how cybersecurity may be seen in terms of systemic risk, how it could be defined and analyzed, and which institutions and countries are most relevant to systemic cyber risk and mitigation.

Researcher Fellows
Conor Cunningham
Cynthia Hannon
Mariam Malik
Rachel Paik
Rishi Paramesh
Heidi Samford
Kunat Sangcharoenvanakul
Sarah Sanguinet
Alison Wattles

Senior Research Fellow
Alexander Wirth

Program Manager
Allison Anderson

Faculty Lead
Jessica L. Beyer

Contact: Jessica L. Beyer, jlbeyer@uw.edu

Table of Contents

Executive Summary

This report analyzes regulatory regimes for international financial services and mechanisms for addressing systemic financial risk in order to identify approaches to the formation of an international regime that could manage systemic risk within the realm of cybersecurity. Additionally, it provides insight into the best practices of financial regulatory regimes and suggests the possibility of future international cybersecurity regulation.

The report articulates financial systemic risk as the possibility that the failure of a component of a financial institution will result in a large-scale failure within the financial sector. The principle of systemic risk is analogous to cybersecurity in that the failure of one component of cybersecurity infrastructure may trigger larger-scale failures including the collapse of critical infrastructure.

To determine how systemic cyber risk may be addressed, this paper analyzes and assesses various regulatory measures used or proposed in the financial sector. We suggest how models to address financial risk may be transposed into potential models to mitigate systemic cyber risk. Specifically, we suggest that the indicators of systemic financial risk developed in the Third Basel Accord can be transposed to systemic cyber risk, as well as methods such as stress testing to measure resilience, limiting damage, and systemic risk taxation.

Examining the institutions that exist in the financial sector to mitigate systemic financial risk can provide examples of potential strategies to mitigate systemic cyber risk. We examine institutions that play roles in the mitigation of systemic financial risk, such as the Federal Reserve and the Financial Stability Board, and suggest that similar institutions could act in the realm of cybersecurity.

Next, we identify potential stakeholders important to the formation and promotion of a future cybersecurity regulatory regime. These stakeholders include governments, militaries, intelligence agencies, Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Organizations (ISAOs), Information Sharing and Analysis Centers (ISACs), law enforcement agencies, civilian regulatory agencies, private industry, intergovernmental organizations (IGOs), and non-governmental organizations (NGOs). Some countries and international stakeholders, such as member states on the United Nations Security Council (UNSC), or the International Monetary Fund (IMF), have already had some involvement in

influencing international cybersecurity policies and are in a position to drive a potential international regime.

Finally, by identifying best practices of existing regulatory regimes managing systemic risk, this paper articulates the potential future of cybersecurity regulation. Some of these best practices include publishing policy decisions, implementing systemic risk authorities, filling regulatory gaps, cooperating internationally and maintaining global regulatory standards.

Articulating Systemic Risk in the Financial Sector and Cybersecurity

What is Financial Risk?

Systemic risk is the possibility that one or a series of events could result in the large-scale failure of a sector, industry, or economy.[1] Financial systemic risk can impact a broad variety of stakeholders given its international nature and connection to other sections of the global economy.

The most recent example of financial systemic failure is the 2008 global financial crisis, where the excessive trading of risk associated with mortgage-backed securities led to a series of bank failures and a global economic recession. While the 2008 crisis was unique in the nature and the scale of its impact on the global financial system, the crisis help illustrates the methods with which stakeholders assess systemic financial risk around the world.

A variety of factors can inform a country or an actor's propensity to generate systemic financial risk from economic to political to societal to geopolitical factors. Domestic macroeconomic risks can include risks associated with lending in volatile economies or political environments, such as what occurred during the 1997 Asian Financial Crisis.[2] Sovereign risk arises from long-term deficits that a country must pay when a crisis is occurring. Transfer risk occurs when a government cannot make payments in foreign currencies.

Politically, the presence of corruption in a society, the role of military in politics, ethnic and religious tensions, effectiveness of laws and bureaucracies, transparency, and accountability are all elements that factor into systemic financial risk.[3] Internal conflicts that threaten the legitimacy of government institutions such as threats of civil war or disorder, coups, violence, and terrorism are all societal issues that can translate into significant economic threats. External threats such as foreign conflicts or pressure contribute to this as well.

---

[1] Borio, Claudio. "Rediscovering the Macroeconomic Roots of Financial Stability Policy: Journey, Challenges, and a Way Forward." *Annual Review of Financial Economics* 3, no. 1 (December 2011): 87–117. https://doi.org/10.1146/annurev-financial-102710-144819.

[2] "Managing Country Risks: Perspectives for the Post-Crisis Landscape." Oliver Wyman. Accessed April 30, 2018. http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/insights/financial-services/2014/WebsiteUpdates/Managing+Country+Risks%20Update.pdf.

[3] "International Country Risk Guide Methodology." The PRS Group. Accessed April 30, 2018. https://www.prsgroup.com/wp-content/uploads/2012/11/icrgmethodology.pdf.

Analyzing Cyber Risk

Like systemic financial risk, the technology sector and its associated cybersecurity components are deeply interconnected and span a broad variety of countries and industries. Systemic cyber risk can be viewed as the probability of an incident or incidents occurring to an individual actor within the technology sector triggering a larger and catastrophic failure of the entire technology sector. Like systemic financial risk, an unstable financial or political environment can also negatively impact the technology sector. Additionally, systemic cyber risk can also be impacted by other factors, such as infrastructure integrity and cyberattacks. Each of these risks have different impacts, but quantifying them is important for controlling major fluctuations in the realm of cybersecurity. Different risks, such as cybercrime or nation-state attack, should be weighed differently when calculating overall systemic cyber risk.

Case Study: 2016 Ukrainian Electrical Grid Cyberattack

The technology sector is particularly heavily reliant on the integrity of critical infrastructure. In 2016, elements of Ukraine's critical infrastructure were impacted through an attack on its electrical grid. In that attack, hackers simultaneously disabled dozens of power substations, leaving over 230,000 Ukrainians without power for as many as six hours.[4]

The hackers were also able to disable backup power generators at two out of the three main distribution centers, which kept operators from manually turning substations back on and launched a telephone denial of service attack against customer call centers to prevent customers from reporting outages.[5] They also replaced legitimate firmware with malicious firmware and were able to wipe files from operator stations, which made many of these substations inoperable for months after the attacks.[6]

Later investigations showed that the attacks began months in advance through a spear-phishing campaign that targeted IT staff and administrators working at Ukrainian power distribution companies.[7] The cyberattacks on the Ukrainian electrical grid were the first of their kind in terms of scope and scale, and serve as an illustration of connection between critical infrastructure, cybersecurity and systemic cyber risk.

---

[4] "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." WIRED. Accessed April 29, 2018. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[5] Ibid.
[6] Ibid.
[7] Ibid.

Regulatory Regime Models

Cyber and Financial Systemic Risk Management

In an increasingly interconnected world, systemic sector risk will continue to pose a major threat to global institutions and industry. This section will analyze how systemic risk is measured in finance and provides a potential analogy for a hypothetical systemic cyber risk regulatory regime. Since the 2008 financial crisis, policymakers have implemented various policy changes in order to reduce the potential of systemic risk within the financial sector.[8] This section will examine some of those changes as well as proposed changes to the financial sector to better mitigate systemic risk. Consequently, we will evaluate each measure's effectiveness and suitability to be transposed to the mitigation of systemic cyber risks. We will discuss three major regulatory measures: stress testing, the provisions of the Third Basel Accord, and systemic risk taxation.

Transposing Systemic Risk Models in Financial Institutions to Cybersecurity

The financial sector uses several models to quantify and measure systemic risk within its sector. The Basel Committee on Banking Supervision and the Financial Stability Board developed a test to calculate the systemic financial risk individual banks contribute to the market that provides a holistic approach to the risk each bank contributes.[9] Table 1 captures the inputs used by the test to measure systemic risk.

[8] World Economic Forum, "How Can We Control Systemic Risk? | World Economic Forum," August 10, 2015, https://www.weforum.org/agenda/2015/08/how-can-we-control-systemic-risk/.
[9] Basel Committee on Banking Supervision, ed., *The G-SIB Assessment Methodology: Score Calculation*, Nov. 2014 (Basel: Bank for International Settlements, 2014).

Table 1: The Basel Committee on Banking Supervision and Financial Stability Board Test

Indicator	Description
Size	A comprehensive measure to show a bank's total exposure and used to calculate the bank's leverage ratio under Basel III.
Interconnectedness	Measures the ability for banks to meet their payment obligations, which are their total claims on the financial system, total liabilities in the financial system, and the total value of debt and equity securities issued by a bank.
Substitutability	Measures how important the provided bank's services are, and how difficult it is for a customer to replace its services if the bank failed.
Complexity	Observes the bank's operations to see whether they are practicing complex operations, which can hinder ease of recovery in case of failure.
Cross-jurisdictional activity	Evaluates the international operations of a bank. There needs to be compliance with various national regulators in the event that a bank fails.

While the Basel Committee on Banking Supervision does not publish the results of its tests, a study conducted by the US Office of Financial Research follows the indicators developed by the Basel Committee to evaluate 33 US banks. Of the eight banks classified as "Globally – Systemically Important Banks" that were put through the test, five of them had "particularly high contagion index values."[10]

The indicators of systemic financial risk, developed under Basel III, could be modified to describe systemic cyber risk. Table 2 below demonstrates how to potentially transpose definitions.

Table 2: Modification of Basel III Systemic Risk Indicators for Cybersecurity

Indicator	Cyber Risk Description
Size	Measures an organization's total exposure and used to calculate how much data an organization holds (a cybersecurity expenditure ratio).
Interconnectedness	Measures the ability for institutions to meet their security obligations, which are their total claims on data, total liabilities in the cybersecurity system, and the total value of data held by an institution.
Substitutability	Measures how important services provided are and how difficult it is for a customer to replace services if the organization failed.
Complexity	Observes the institution's operation to see whether they are practicing complex operations.
Cross-jurisdictional activity	Evaluates the international operations of an institution. There would need to be compliance with various national regulators in the event that an institution or its data centers fail.

[10] Meraj Allahrakha, Paul Glasserman, and H Peyton Young, "Systemic Importance Indicators for 33 U.S. Bank Holding Companies: An Overview of Recent Data," February 12, 2015, 7.

The work established here provides several ideas for how to transpose financial models and analysis to cybersecurity. In the next subsections, we examine the regulatory regimes that are in effect or part of the financial systemic risk discourse, and examine how they might be transposed into a cybersecurity setting. We discuss the use of stress testing, ways to limit damage, and taxation specifically. The Office of Financial Research argues that a cybersecurity failure could lead to negative effects in the financial sector through the lack of substitutability, the loss of confidence, and loss of data integrity.[11]

Regulation and Taxation to Address Systemic Financial Risk

This section outlines three areas of "lessons learned" from the area of systemic financial risk and how such methods could be applied to systemic cybersecurity risk. These three areas are the use of Comprehensive Capital Analysis and Review stress testing techniques and other related methods to understand how a bank will respond under extreme stress, the Basel III damage control regulations, and the use of systemic risk taxation.

Lessons from the Comprehensive Capital Analysis and Review: Stress Testing

The Dodd-Frank Wall Street Reform Act of 2010 introduced a new annual stress test requirement for banks under the Comprehensive Capital Analysis and Review (CCAR). This stress test helps to ensure that there are sufficient and adequate capital holdings within an individual bank in the event that the bank is put under extreme stress. Therefore, banks are evaluated through scenarios of economic downturn and assessed on how economic downturn affects the bank's functions. These scenarios can vary from an unexpected downturn of economic activity to a major bank failure. Stress testing may vary from year to year as it examines simulated bank performance through the current state of the economy.[12]

In addition to traditional stress testing, the Agent-Based Model, which runs repeated simulations of interactions between different agents to gain insight systemic risk, is widely used

[11] The Office of Financial Research, "Cybersecurity and Financial Stability: Risks and Resilience," February 15, 2017, 12.
[12] Venetia Woo, Bharat Chelluboina, and Wilfrid Xoual, "The Effectiveness of the Regulatory Stress Testing Disclosure Process," Financial Markets, Institutions & Instruments 23, no. 1 (February 1, 2014): 1–70, https://doi.org/10.1111/fmii.12014.

to study risk in the financial sector and shows potential to be used for stress testing.[13] The model can examine possible scenarios each individual stakeholder will take if there is a change within a system. For example, it can simulate how much a bank is willing to engage in a high-risk transaction when there is a systemic risk tax. This model can provide insight to economists who are trying to study the consequences of systemic financial risk.[14] Therefore, this model is a possible method in the cyber realm to practice and evaluate processes for regime construction.

Stress tests have shown to be an effective method to ensure economic stability in the finance sector if the tests are rigorous enough.[15] Stress testing could become an effective tool to ensure systemic stability in the cyber realm as well. For example, annual stress tests could be conducted for tech sector organizations that are considered to be critical to global cyber stability. Scenarios could include a simulation of a large cyberattack on a data center that could put operations at risk, or the effects of failure in data centers and how the organization copes with subsequent externalities. Through stress tests, organizations are evaluated on their ability to securely protect data and how they can mitigate threats towards that protection.

This is not to say that stress testing is without flaws—the central question is weighing between having astute systemic security or only complying with the law. Prior to the 2008 financial crisis, stress tests had already been introduced to the financial sector.[16] However, stress testing was found to be ineffective in mitigating systemic risk, due to the lenient and complacent regulations for financial institutes. The ineffectiveness of stress testing prior to 2008 underlines the importance of not having stress tests only for static compliance measures, but rather, as a dynamic measure in which the main goal of the test should be aiming for greater systemic cybersecurity. Therefore, there should be a standardized measure for these audits, similarly, to System and Organization Control reporting (SOC) audits.[17] These audits should provide stakeholders with confidence that the audits conducted are stable and secure.

---

[13] John Hill, "Using Agent Based Models for Stress Testing," Simudyne (blog), February 8, 2018, https://medium.com/simudyne/agent-based-models-for-stress-testing-f8430ed43cdc.
[14] OECD, Systemic Financial Risk, OECD Reviews of Risk Management Policies (OECD Publishing, 2012), https://doi.org/10.1787/9789264167711-en.
[15] Woo, Chelluboina, and Xoual, "The Effectiveness of the Regulatory Stress Testing Disclosure Process."
[16] Woo, Chelluboina, and Xoual.
[17] PricewaterhouseCoopers, "System and Organization Controls (SOC) Reporting," PwC, accessed May 10, 2018, https://www.pwc.com/us/en/services/risk-assurance/third-party-assurance/soc-reporting.html

Lessons from the Third Basel Accord: Limiting Damage

The Basel Committee on Banking Supervision published the Third Basel Accord (Basel III) in 2009, building on two previous accords. Basel III aims to improve from the previous two accords by helping banks better mitigate the systemic failure, such as the failure of Lehman Brothers in the 2008 crisis. The accord seeks to improve the banks' ability to cope with increased stress, improve its risk management, and increase transparency. Overall, it addresses the issues by increasing capital requirements and lowering a bank's leverage. This does not necessarily reduce the risk of a bank failing, but rather limits the damage the bank causes to the financial system when it fails.[18]

Basel III imposes two central conditions to address the potential damage of a bank failing: capital requirements and liquidity and leverage ratios. In relation to capital requirements, Basel III includes stricter capital requirements than its predecessors. Therefore, during credit expansions, banks need more capital to set aside. Large, important banks are subject to higher capital requirements as a counter-cyclical measure. In relation to liquidity and leverage ratios, Basil II introduces these two ratios as a preventative measure against disproportionate levels of leverage by restricting banks from excessive borrowing and ensuring sufficient liquidity within banks to address potential financial stress.

These two factors secure a bank's ability to remain solvent. A leverage ratio requirement can reduce the risk of a "bank run," reducing that type of financial systemic risk.[19] With a leveraged ratio requirement, assets and collateralized debt obligation must exceed their liability on the balance sheet and preserve equity. Since a bank's assets become more liquidated, this means that a bank can pay off their debt in a timely manner. Hence, systemic risk is reduced as banks can persevere if one of the banks deemed "too big to fail" actually fails. Additionally, a study published by European Financial Management concluded that having a liquidity coverage ratio increases a bank's financial stability while providing an indicator on the stability of a bank.[20]

---

[18] "Basel III: International Regulatory Framework for Banks," December 7, 2017, https://www.bis.org/bcbs/basel3.htm.
[19] Jean Dermine, "Basel III Leverage Ratio Requirement and the Probability of Bank Runs," Journal of Banking & Finance 53 (April 1, 2015): 266–77, https://doi.org/10.1016/j.jbankfin.2014.12.007.
[20] Brian Du, "How Useful Is Basel III's Liquidity Coverage Ratio? Evidence From US Bank Holding Companies," European Financial Management 23, no. 5 (October 1, 2017): 902–19, https://doi.org/10.1111/eufm.12116.

To transpose Basel III to the cybersecurity, it is crucial to understand the differences between the financial and cybersecurity sector. The regulatory aspects of Basel III need to be adjusted to meet the demands of cybersecurity. The regulation proposals for the cybersecurity realm are as follows:

- **Transparency Requirement:** This requirement aims to act proactively. Regular stress test audits must be conducted in collaboration with the cybersecurity systems of tech sector organizations. Organizations that are global systemically important should be subject to stricter standards.
- **Cybersecurity Expenditure Ratio:** This ratio aims to increase expenditure on cybersecurity. This means that a portion of revenue each year should be utilized to improve defensive cybersecurity, including preparing for stress test audits. Additionally, global systemically important entities could be subject to higher cybersecurity expenditure ratios.

These regulatory requirement proposals are derived from our research, which notes the importance of transparency and security to mitigate systemic cyber risk. As technology institutions expand, stress test audits could be crucial to discovering flaws in cybersecurity measures. Institutions can then address flaws within their system through the cybersecurity expenditure ratio requirement. These requirements should assist in reducing systemic cyber risk.

Global systemically important organizations would be subject to higher requirements because larger institutions are inherently more prone to systemic cyber risk, since their operations are generally larger, more complex, and more difficult to replace in an outage event. Hence, it is crucial to address organization size with stricter requirements for mitigation efforts to become effective.[21] These requirements are both proactive actions to maintain regular cybersecurity and to reduce the possibilities of systemic cyber risk. However, providing a regulation that many stakeholders must comply with can be challenging as witnessed in this Basel III Accord. Many changes and delays have affected the implementation of Basel III due to disagreements between both private and state actors. There are encouraging signs that as G20

[21] Woo, Chelluboina, and Xoual, "The Effectiveness of the Regulatory Stress Testing Disclosure Process."

nations pledge to work towards a more secure cyber realm. This is including China, where the state had been scrutinized for exploiting intellectual property of other actors.[22]

Lessons from Pigouvian Taxes: Systemic Risk Taxation

Another approach to mitigate financial systemic risk is Pigouvian taxes. Pigouvian taxes are taxes on market activity that generates negative externalities to correct inefficiencies within the market, such as an increase in systemic risk. For example, financial transactions that are regarded as contributing to increasing financial systemic risk would be subject to transactional taxation.[23] A "systemic risk tax" known as the "financial responsibility fee" was introduced in the United States in 2011, although it has not been implemented.[24] The tax revenue collected from a systemic risk tax would be used to assist in the bailing out of a bank in a failure. In the US, this is called the Troubled Asset Relief Program, and was introduced specifically to address the 2008 crisis.

Systemic risk taxes are widely advocated as an alternative to the Basel III regulatory framework, since they do not hinder the ability for banks to borrow and, thus, carry a greater chance of economic stimulation. Systemic risk taxes have been shown to significantly reduce the overall volume of high-risk trades by discouraging bank behaviors that lead to greater systemic risk. [25]

A similar tax could be built into the cybersecurity sector, meaning that institutions would not put data at risk without serious cause. To implement a tax, our measurements of systemic cyber risk would have to be widely accepted, to make quantifying taxation possible. The tax revenue would be allocated to an organization that is responsible for monitoring systemic cyber risk. If the tax revenue was used to bail out failures in organizations, the decreased risk of failure could prove to increase systemic cyber risk. Multiple countries would need to be on board with

---

[22] Williams, Katie Bo "G20 Nations Reach Anti-Hacking Pledge," Text, The Hill, November 17, 2015, http://thehill.com/policy/cybersecurity/260414-g20-nations-reach-anti-hacking-pledge

[23] Donato Masciandaro and Francesco Passarelli, "Financial Systemic Risk: Taxation or Regulation?," Journal of Banking & Finance 37, no. 2 (February 1, 2013): 587–96, https://doi.org/10.1016/j.jbankfin.2012.09.020.

[24] Douglas J. Elliott, "The Proposed 'Financial Crisis Responsibility Fee,'" Brookings (blog), May 11, 2010, https://www.brookings.edu/testimonies/the-proposed-financial-crisis-responsibility-fee/.

[25] Sebastian Poledna, Olaf Bochmann, and Stefan Thurner, "Basel III Capital Surcharges for G-SIBs Are Far Less Effective in Managing Systemic Risk in Comparison to Network-Based, Systemic Risk-Dependent Financial Transaction Taxes," Journal of Economic Dynamics and Control 77 (April 1, 2017): 230–46, https://doi.org/10.1016/j.jedc.2017.02.004.

taxes, so organizations could not move their operations to locations outside of the taxation jurisdiction.

It is not clear how well a systemic risk tax would work in the cyber realm. While the financial sector carries huge amounts of taxable transactions, this is not the nature of the cyber sector. Since there is not a clear way to tax the technology sector, or a clear institution to implement taxation, systemic risk taxes may be less suitable for systemic cyber risk. This is because, there are more factors that are needed to be agreed on, when compared to implementing a regulatory regime similarly to Basel III.

Evaluating Institutions and Regulatory Regimes

Financial Institutions and Regulatory Regimes

Examining systemic risk management within the financial sector and its institutions can be useful in creating a regime to meant manage systemic cyber risk. There are a number of institutions and regulatory regimes in the financial sector, most of which were established following financial crises (e.g., Federal Reserve was established after the Panic of 1907 and the Financial Stability Board was reformed after the 2008 crisis) that cybersecurity policymakers could use as examples for systemic cyber risk.

These institutions strive to achieve roughly the same goal—creating a safe banking system internationally or domestically that promotes economic development and growth. In terms of financial systemic risk, all financial institutions and regulatory regimes address the matter in some way, especially following the 2008 crisis.

Central Banks

A central bank provides financial services and implements monetary policy for its nation's government and banking system. Central banks must be transparent to maintain credibility in front of the public. Transparency not only strengthens the effectiveness of monetary policy by providing expectations of the future, but also holds central banks accountable for their actions. Instead of tying monetary policy to specific predictive models, policymakers must inform the public of a multitude of economic forecast methods used to inform policy. For instance, the Federal Open Market Committee[26] releases a statement of prospective policy and its reasoning, holds a press conference to answer questions, publishes Federal Open Market Committee meeting minutes, and gives the public access to its Monetary Policy Report.[27]

Additionally, some central banks (such as the European Central Bank) argue they should be financially independent and have ensured long-term profitability in order to mitigate systemic financial risk. Financial independence is crucial in maintaining a central bank's sovereignty for implementing monetary policy. Ensured long-term profitability combats the effect that short-term profit or loss has on a central bank's policy decisions.

[26] The Federal Open Market Committee is a high-profile committee within the Fed that meets eight times per year.
[27] "Challenges Associated with Using Rules to Make Monetary Policy."

Establishing healthy reputations, holding central banks accountable for their actions, financial independence, and long-term profitability can all be transposed onto the field of cybersecurity. Because of the nature of cybersecurity, creating a system for accountability in the cyber realm is more difficult than in the financial sector. However, a system of transparency and accountability are two very important aspects that can be transposed into cybersecurity. Transparency and best-practice sharing in cybersecurity policy could be an important way to boost risk mitigation tactics. Transparency in cybersecurity policy can raise awareness of cybersecurity best practices among the public and serve as a way to hold companies accountable to their peer standards.

Systemic cyber risk continues to increase as the world grows more connected. Financial independence has proven to be very valuable when mitigating financial risk. Because of the nature of the cyber realm, where we see a continual increase in dependence and integration rather than independence, independence appears increasingly improbable as the choke points such as data centers increase in number and become more greatly integrated. Therefore, making cybersecurity a priority and setting standards for private sector entities is a far more probable method to mitigate systemic cyber risk.

Government Agencies

Government agencies, such as the Securities and Exchange Commission and Commodity Futures Trading Commission, are created by governments to mitigate financial risk. For example, the Securities and Exchange Commission was created to protect investors by promoting transparency in the financial sector.[28] The Commodity Futures Trading Commission polices the derivatives market for abuse, overseeing more than $400 trillion in the swaps market—a market that played a key role in the 2008 financial crisis.[29] These two government agencies utilize specific systemic risk management tactics by promoting transparency to increase public trust and policing markets that could carry financial systemic risk.

Transposing government agencies from the financial sector to cybersecurity could be a valuable technique to mitigate systemic cyber risk. Potential government agencies analogous to

[28] "About the SEC." *U.S. Securities and Exchange Commissio*n. 100 F Street, NE Washington, DC, 2017. Accessed April 29, 2018. https://www.sec.gov/about.shtml.
[29] "Mission & Responsibilities | U.S. COMMODITY FUTURES TRADING COMMISSION." *U.S. COMMODITY FUTURES TRADING COMMISSION*. Accessed April 20, 2018. https://www.cftc.gov/About/MissionResponsibilities/index.htm.

the Securities and Exchange Commission and Commodity Futures Trading Commission could work in a similar way to mitigate potential systemic threats. New government agencies could work to implement guidelines and standards set forth by the National Institute for Standards and Technology (NIST) as protocols for the private sector. Agencies could provide incentives through fines and other repercussions to companies and banks to adhere to standards that would reduce the systemic cyber risk.

International Organizations

International organizations within the financial sector aim to provide a framework for its members to further strengthen global financial systems. Organizations such as the International Monetary Fund (IMF), the Bank for International Settlements, the Organization for Economic Co-operation and Development, the Financial Stability Board, and the European Commission all focus on economic development, promoting financial stability, facilitating monetary policy, filling regulatory gaps, and mitigating systemic risk. Furthermore, international cooperation and collaboration is crucial when implementing standards that encompass international financial organization mandates. These organizations collaborate via conferences and summits in order to develop a cohesive, international financial system.

In May 2010, the IMF organized a conference in Washington D.C., called the Conference on Operationalizing Systemic Risk Monitoring, addressing systemic risk within the financial sector.[30] The conference covered potential ways to identify new Systemically Important Financial Institutions, Markets, and Instruments that would qualify for systemic risk regulation. Identifying institutions that are systemically important is crucial in mitigating risk, as regulation is made more stringent for Systemically Important Financial Institutions, Markets, and Instruments whose collapses can compromise the financial system.

The possibility of stand-alone systemic risk regulatory authority was discussed within the conference.[31] As systemic risk continues to pose serious threats to the financial sector, efforts to prevent risk or alleviate its effects are crucial to financial stability. Dedicating financial institutions entirely to mitigating risk would help focus and refine systemic risk management.

---

[30] "Conference on Operationalizing Systemic Risk Monitoring, May 26–28, 2010 Washington, DC." *IMF*. 700 19th Street, N.W., Washington, D.C. 20431, 2010. Accessed April 13, 2018. http://www.imf.org/external/np/seminars/eng/2010/mcm/.

[31] Ibid.

The conference also addressed the failure of standard metrics for households, corporate actors, and municipalities to raise warning prior to the financial crisis, in part due to the increased use of derivatives.[32] The lack of regulation seen in the derivatives market was an enormous regulatory gap that not only highly disrupted the financial market, but also went largely unnoticed until it was much too late.

The creation of international institutions to assist in systemic cyber risk mitigation could be an important aspect to global cybersecurity in the future. Though many of the aforementioned financial aspects in this section are non-transposable to cybersecurity, financial institutions do provide a more general idea of what components of systemic cyber risk should be potentially addressed by institutions in the future. Organizations analogous to institutions such as the IMF could play an important role in developing norms and creating a platform for international cooperation on risk mitigation. Developing standards, guidelines, and goals for vital private sector entities to adapt and continue to develop will work to mitigate systemic risk much as it has in the financial sector. Gatherings such as the Conference on Operationalizing Systemic Risk Monitoring could be an area of the financial sector that could be reproduced for cybersecurity. A hypothetical cyber conference could discuss systemic risk in cybersecurity and identify vital stakeholder for systemic risk mitigation.

Cybersecurity policymakers can learn a lot from institutions within the financial sector. The field of cybersecurity is at an advantage in managing systemic risk before a crisis occurs similar to those encountered by the financial sector. Promoting transparency, establishing credibility, filling regulatory gaps, cooperating internationally, maintaining global regulatory standards and directly focusing on systemic risk are tactics cybersecurity institutions can look to in developing a framework for mitigating risk.

[32] Ibid.

Drivers of a Potential International Cyber Regime

The identification of stakeholders and their importance in creating a strong international cyber regulatory regime is vital in mitigating cyber systemic risk. The public and private sector both have a role to play in ensuring better cyber regulation. The government, through legislation regulatory agencies and law enforcement, are fundamental in the development of a cyber regime, while also carrying a unique suite of interests in their military and national security apparatus. In addition, the private sector, where firms vary in size and role in the technology sector, can benefit and aid in creating a strong regime by working with the public sector and other private entities such as NGOs or IGOs. All sectors often share the common interests of the protection of data, civil liberties, intellectual property, reputation, revenue, and a robust economic sector. Building cyber resilience should, therefore, be a joint effort between all relevant actors.

Public Sector

In a hypothetical cybersecurity regime, national regulatory agencies will play an important role in creating standards and encouraging cyber resilient practices. This responsibility will likely belong to national agencies that regulate trade and commerce as well as agencies that manage industry and critical infrastructure. While government cybersecurity interests are often intertwined with the interests of the private sector, government motivation is less tied up in profit motivations—and more focused on security, protection of foundational rights (such as those in the US Constitution and Bill of Rights), ability to regulate private enterprise, and public safety.

Government

In the United States, the Department of Homeland Security (DHS) and the Department of Commerce (DOC) work with intelligence agencies such as the Federal Bureau of Investigation (FBI) to identify, mitigate, and manage cyber risk. Within the DOC is a unique measurement agency called the National Institute for Standards and Technology (NIST) which, while not a regulatory agency, plays an important role in cybersecurity by defining, supporting, and promoting standards for cyber resilience in the private sector. In 2014, the Cybersecurity Enhancement Act (CEA) updated the role of NIST to "facilitate and support the development of"

cybersecurity risk frameworks. Through the CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."[33] By setting up frameworks for private companies within critical infrastructure sectors to follow, NIST was able to encourage the private sector to enact cyber resilient practices. In other countries, national government agencies may follow NIST's approach to cybersecurity in risk mitigation.

According to the NIST's cybersecurity framework, cyber risks put the nation's security, economy, and public safety and health at risk. Therefore, a government's primary interest in cyber regulation is to protect national critical infrastructure but also to be able to identify, mitigate, and manage cyber risks. The Patriot Act of 2001 defines critical infrastructure as:

> Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[34]

In addition, the US Department of Homeland Security defines 16 different critical infrastructure sectors within the United States, including chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare & public health, information technology, nuclear reactors, materials, and waste, transportation systems and water and wastewater systems."[35] Each of these critical infrastructure sectors would be a stakeholder in larger systemic cyber risk. Because of their diversity, the preferences of each stakeholder group are difficult to infer and would vary depending on the country. The ownership of these sectors within critical infrastructure is not always private, which would likely make it easier to implement cybersecurity measures in those sectors.

The reliability of national critical infrastructure remains important not only to maintain the public trust, but also for that government to attract foreign investment and retain domestic firms. As a result, a government is liable to protect the stakeholder interests of both its public and its private sector. In the same way, we imagine that an international cyber regime that manages

[33] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0."
[34] Ibid.
[35] "Presidential Policy Directive -- Critical Infrastructure Security and Resilience."

systemic risk would have to consider similar stakeholder interests, both public and private, that make up critical infrastructure in each nation.

Military

Militaries are an important facet to many security apparatus, and would likely be a stakeholder in a given cyber regime. The military's capabilities rely on the stability of their systems to monitor risks, and coordinate efforts critical to national security and political stability. The increase of cyber risk has caused militaries to expand their capabilities to defend against external cyber threats. When threats from overseas become severe, they may be elevated from law enforcement agencies to the military for response.[36] However, the umbrella of information security applies to civilian systems that may not affect national security, and is often considered to be outside of the scope of a military's responsibility.

In addition, the military's own reliance on networks and computer systems makes it vulnerable to critical failures. Therefore, determining the role of the military within cybersecurity is a challenge, and the primary role of military in cybersecurity is not necessarily to defend information systems within a country but rather to protect their own critical systems and to develop a capacity for offensive cyber operations.[37] The expansion of "civil contingencies" programs and public private partnerships may be of interest to the military in order to provide an avenue for protection of civilian information systems.[38] Militaries have an interest in preparedness to retaliate and deter offensive cyberattacks and to protect their intelligence networks, and may participate in international regimes through information sharing and cooperation with allies, as in conventional warfare, and use cyber warfare as a supplement to other components of warfare. The most important priority of a military is to improve their own system's defense and resilience, because of the challenge of deterring and attributing cyberattacks.

While some level of cooperation and involvement from a military would be expected and necessary in an international cyber regime, militaries also have an interest in maintaining some level of operational autonomy and information protection from even the closest allies.

---

[36] Wallace, Ian. "The Military Role in National Cybersecurity Governance." *Brookings* (blog), November 30, 2001. https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/.
[37] Peter Sommer, and Ian Brown. *Future Global Shocks*. OECD Reviews of Risk Management Policies. OECD Publishing, 2011. https://doi.org/10.1787/9789264114586-en.
[38] Ibid, p. 13

International regulations must provide states with the freedom to conduct their own military operations to address their own vulnerabilities and emerging risks. Overall, the military will support international cyber policies that address global cyber incident response in a way that does not conflict with national security interests, and may provide support for an international treaty similar to the Nuclear Non-Proliferation Treaty, but aimed to limit the use of cyber warfare and aid the formation of national cyberattack entities.[39]

Intelligence Agencies

Intelligence agencies have an interest in both determining emerging cyber threats and in performing espionage in the cyber realm to access intelligence information. Intelligence agencies monitor cyber activity to identify current or emerging cyber incidents against both civilian and government entities to guard intellectual property, technology, and vital information and services. Intelligence agencies have an interest in determining a structure for cybersecurity both domestically and internationally, as well as in early detection of cyberattacks and the formation of an effective deterrence strategy.[40]These agencies could clearly benefit from the information sharing and trust building that an international cyber regime would require.

While intelligence agencies are able to notify organizations of potential risks and encourage further development of their security procedures, there is concern over a conflict of interest in that intelligence agencies are both aimed to protect information systems and critical services as well as develop offensive cyber weaponry that might be the cause of a major cybersecurity system level event.[41] This conflict of interest results in information asymmetry between the intelligence agencies, the government, companies, and individuals. Companies across sectors find this to be frustrating, as they could better protect themselves from and respond to cyber incidents if there was increased information sharing between intelligence agencies and Internet users. However, a delay or lack of information filtration from intelligence agencies to Internet users can be a strategic choice to aid in the function of intelligence agencies.

---

[39] Ibid, p. 63, 84

[40] "Cyber Security and the Intelligence Community | Belfer Center for Science and International Affairs." Accessed April 29, 2018. https://www.belfercenter.org/publication/cyber-security-and-intelligence-community.

[41] "Take Cybersecurity Away From Spies - For Everyone's Sake." Chatham House. Accessed April 29, 2018. https://www.chathamhouse.org//node/31614.

Computer Emergency Response Teams

Many governments have responded to the growth of cyber threats by implementing national cybersecurity policies. These policies help to mitigate cyber risk, promote stable information infrastructure, and often share information internationally to build national capacity to resist and respond to cyber incidents.[42] A common and fundamental cornerstone of national cybersecurity strategies and the national security apparatus are Computer Emergency Response Teams (CERTs) also known as Computer Security Incident Response Teams (CSIRTs), which participate in the Forum for Internet Response and Security Teams. The Forum for Internet Response and Security Teams provides an avenue for entities in different countries to build trust and collaborate to resolve problems quickly and efficiently. Because of this, the Forum for Internet Response and Security Teams is able to play a helpful, yet informal role, in the security apparatus. The structure of CERTs/FIRST is currently the only recognized mechanism for international governance of cyber incidents.[43]

The primary goal of a CERT is to protect networked systems by resisting cyber incidents and responding to cyberattacks in a way that mitigates damage and allows for continuity of critical services. A CERT's response may be reactive or proactive, involving both mitigation and prevention.[44] Reactive services often include alerts and incident handling in addition to warnings. Proactive services include security assessments, the development of security tools or corrections, and intrusion detection. Countries with established and capable cybersecurity regimes tend to have multiple CSIRTs.

The most advanced or mature CERTs have a broad set of capabilities and play a role in national and transnational CERT communities, because CERTs operating at the national level are responsible for acting as a point of contact for cybersecurity issues. Such cooperation can exist bilaterally between two CERTs, within associations of CERTs concerning specific goals or regions, and between associations of CERTs. In these arenas, CERTs cooperate in responding to incidents and share information and best practices to improve the overall efficiency and

---

[42] Shamir B. Hashim, Mohd. "Malaysia's National Cyber Security Policy: The Country's Cyber Defence Initiatives." *Cybersecurity Summit (WCS), 2011 Second Worldwide*, 2011, p. 6.
[43] Sommer and Brown, 2011, p.85.
[44] Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. 2015. *CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams*. Working paper. *CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams*. New America; The Global Public Policy Institute. Available from https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT Basics for Policy-Makers.7694665e821048ef85a6007eb5a29105.pdf.

effectiveness of their security efforts. Some states with mature CSIRTs have created national bodies to govern the activities of CSIRTs and are increasingly supporting the development and improvement of other CSIRTs through information sharing and training.[45]

Moreover, CERTs are coordinate responses to computer incidents between cybersecurity stakeholders.[46] This means that they work with a wide range of entities, including individuals, Internet Service Providers, the private sector, development partners, and law enforcement. A good candidate country for cyber investment, or a country that may be able to lead an international cyber regime, would ideally have one or more "mature" CERTs, involved in active cooperation within an association of CERTs.

Information Sharing & Analysis Centers

Information Sharing and Analysis Centers (IASCs) and Information Sharing and Analysis Organizations (ISAOs) are also a feature of the US cybersecurity landscape and drive cybersecurity collaboration by facilitating community building, information sharing, and coordinated incident response. The existing ISACs were established at different times (e.g., FS-ISAC in 1999 and Auto-ISAC in 2014) to mitigate risk, respond to cyber incidents, and share information and alerts within their respective sectors, between sectors, and with the government. Within their sectors, for example banking and finance, energy, defense, and telecommunications, ISACs are extremely effective due to their remarkable penetration within their sector, often over 90%.[47] The structure of ISACs could serve as an example and basis for similar information sharing and collaboration within an international regime. In the US, ISAOs were established in 2015 via Executive Order 13691 to promote the formation of ISAC entities for sectors that did not have an ISAC.

Law Enforcement

Law enforcement agencies influence legislation while also serving in an implementation role. Law enforcement agencies can bring together multiple stakeholders to effectively mitigate systemic risk through partnership. An example is through the establishment of task forces. These

---

[45] Ibid.
[46] Ahmad, Rahayu Azlina A., and Mohd Shamir S. Hashim. "The Organisation of Islamic Conference - Computer Emergency Response Team(OIC-CERT): Answering Cross Border Cooperation." *2011 2nd Worldwide Cybersecurity Summit, WCS 2011*, 2011, p. 2.
[47] "ISAOs." Cyber Threat Intelligence Network. Accessed April 29, 2018. http://ctin.us/site/isaos/.

designated groups of experts, compiled from actors from various law enforcement agencies, legal firms, private-sector companies, and scholars, that can be brought together to pool resources for more detailed and analyzed investigations which can help forecast and create more effective cyber policy and aid countries in cyberattack deterrence.[48] The police force is also better able to inform civilians about attacks through ad campaigns and public service announcements.

As local law enforcement around the world becomes more digitized, vital reports, criminal data, and confidential information found in law enforcement agency networks such as the local police are susceptible to breaches. This could include practices such as tampering with evidence or uncovering witness identities.[49] To store and effectively protect that data, local law enforcement institutions heavily benefit by implementing measures to reduce risk.

Law enforcement is also essential in discovering cyber breaches, generally at the forefront of attack identification.[50] This is in part because law enforcement agencies identify risks and cyberattacks when companies, for the sake of their credibility, sometimes do not report such attacks.[51] By doing so, various law enforcement organizations help identify more risks than would go reported, hence reducing the occurrence of systemic cyber risk. Nations with adequate law enforcement are can allocate a higher resource base to improve knowledge, tools and the use of complex and defined cybersecurity measures in law enforcement agencies, which in turn means enacting policy to reduce systemic cyber risk.

Judicial System and Legislation

The judicial and legislative branches in a country are vital to mitigating systemic risk. Transcending physical geopolitical borders, a country's laws must comply with international Internet Governance regimes and any other agreements a country has made.

For instance, in 2014 and 2016 NATO introduced the Enhanced Cyber Defense policy and the Cyber Defense Pledge respectively, in order to enhance resources and information among member states while encouraging and understanding the role of cybersecurity in

[48] Police Executive Research Forum, *The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime,* April 2014, p.17
[49] Melendez, Steven. *Police Departments Are Vulnerable To Cyberthreats As Evidence Goes Digital.* Fastcompany.com. Published 28th January 2016. Accessed April 20, 2018.
[50] As shown through a survey within the U.S. with law enforcement identifying 20% of cyber attacks. Kopp, Emmanuel, Lincoln Kaffenberger, and Christopher Wilson. *Cyber Risk, Market Failures, and Financial Stability.* IMF, Working paper. August 7, 2017, p.5.
[51] Ibid., p.12

collective defense policies. This set a benchmark for the standards of legislation, critical infrastructure protection and cybersecurity capabilities each member state was expected to have for the security of individual members and the alliance as a whole.[52] Such agreements help establish a more defined and compatible legal cyber framework, and cooperation reducing systemic cyber risk.

Domestically, it is important for countries to have strong local cyber laws and introduce initiatives to help local companies, multinational companies and others in the private sector, reduce major breaches and risk. For example, the EU implemented laws for greater enforcement and accountability measures to reduce risk.[53] Local laws can aid firms in reporting cybercrimes through incentives or ensuring confidentiality. ISPs and private companies find it easier to work with governments whose laws are transparent and prioritize privacy as to not lose consumer confidence.[54] More transparent laws and greater accountability also help eliminate corruption, creating more safety and stability.

The greatest problem the rule of law faces in creating laws to prevent risk is contested or sparingly, or ambiguously, defined definitions of cyberattacks, cybersecurity and systemic cyber risks. Desirable states for cloud providers will have well-defined or formally defined definitions of cyber terminology that comply with those used by large intergovernmental or international institutions recognized in formal law and well integrated into local legislation. In defining cyberattacks, countries must identify the varying levels of threats they face and the organization of government cyber agencies into different divisions to help with the investigation, maximization of efficiency of the legal cyber sector and eventual prosecution or political retaliation of such cyberattacks.

Finally, countries must have or suggest laws identifying their role in oversight and partnering with the private sector for better measures.[55] This includes improvement of information sharing between the sectors, giving more protection and security, better incentives and aid in improving workplace education and awareness about cyber threats and risks.

Therefore, like other stakeholder institutions, the willingness of these local law enforcement agencies to enact cybersecurity measures does play a role in determining cyber risk

[52] NATO, NATO Cyber Defence Factsheet, February 2018.
[53] DTCC. *Cyber Risk — A Global Systemic Threat*. October 2014. P.14.
[54] Police Executive Research Forum, 2014, p.25.
[55] DTCC. 2014

and its mitigation, to establish a data center or allow for technological investment. Less corruption means willingness on the part of governments to improve their security practices and ensuring the implementation of measures into the written law. These laws and enforcers, along with a country's ability to have several or mature CERTs, are key stakeholders in eliminating systemic cyber risk.

Private Sector

Major private sector actors would include any company responsible for the storage and transmission of data, the underlying software that data movement is built upon, and any other companies that touch upon data infrastructure including utilities, which can be publicly or privately owned depending on location. These stakeholders can vary in size from small to medium sized businesses, but most critical cybersecurity actors that would be involved in systemic risk are major actors within a given geographical space. Private sector actors are, fundamentally, profit driven and are accountable to a much different set of actors than government. These companies are likely to prefer limited but transparent regulation, limited taxation,[56] protection from nation-state attack and other crisis-level situations, and market stability.

Major companies involved in the storage and transmission of data are cloud computing providers and Internet Service Providers (ISPs). Cloud computing providers, such as Microsoft, Amazon Web Services, and Google, hold massive amounts of data, creating a very high systemic cybersecurity risk. The data centers that underly the cloud are connected into Internet infrastructure controlled by various ISPs. An ISP stakeholder can be defined as any enterprise responsible for the delivery of a connectivity service, an information service, or an application service to the consumer.[57] ISPs are responsible for major elements of Internet users' experience – from security practices meant to protect users to punitive actions for violations against their consumer protocols. ISPs can also suspend of accounts, blocking access to illicit websites, de-prioritization of traffic, blocking/altering transmission of viruses, and pursuing legal actions against violators.

---

[56] Chapman, Ben. "Ireland's Economy Grows 26.3% in 2015 as Corporations Flock to Low Tax Rate | The Independent," July 13, 2016. https://www.independent.co.uk/news/business/news/ireland-s-economy-grows-263-in-2015-as-corporations-flock-to-low-tax-rate-a7133321.html.

[57] Altmann, Jörn. "A Reference Model of Internet Service Provider Businesses." Internet and Mobile Systems Lab, n.d.

Service providers play a large role in the mitigation of cyber risk by incentivizing the creation of more secure products to guard from potential large financial losses. For instance, as Internet of Things (IoT) network usage continues to grow, so does the number of vulnerable entry points into Internet infrastructure and opportunities for a cybersecurity breach. Arbor Network Annual Worldwide Infrastructure Security Report concluded that service providers face rising distributed denial of service (DDoS) attacks at an increased frequency. These attacks cost service providers significantly, with DDoS attacks costing 25% of data center and cloud providers above $100,000, while 5% reported costs of over $1,000,000.[58] Thus, increased coordination between ISPs and law enforcement agencies will aid in addressing potential security risks before they become detrimental to enterprise and company profits. This can occur through best practice sharing, information exchange and the advancement of criminal compliance programs. If CERTs share their classified information regarding security breaches with the ISPs involved, ISPs may become more active members in cyber systemic risk mitigation.

Mobile Service Providers (MSPs) share similar preferences with ISPs, as well as platforms like Microsoft, Google, and Amazon. MSPs are a strategic access point for cyberattack and vulnerable to security breaches and cyber risk. Current MSP "mobile threat defense" mechanisms include scanning for potentially risky apps and threatening WiFi networks that could result in security risks.[59] A breach within MSP systems can result in network congestion, service outage, and information data theft. In order to increase cyber risk resilience, MSPs could institute preventative risk practices with ISPs and engage in interoperability with parallel MSPs to create more stringent security initiatives. Since so much of the world's population is using mobile devices as a primary computing device, MSPs are also a critical stakeholder.

Finally, as discussed in Section 1, the 2016 cyberattacks on the Ukrainian electrical grid illustrate the centrality of utilities to cybersecurity systemic risk. Energy underpins every element of a country's information and communication system making utilities—particularly, power—a

[58] Report, Security. "Arbor Networks' 12th Annual Worldwide Infrastructure Security Report." Arbor Networks®, January 24, 2017. https://www.arbornetworks.com/arbor-networks-12th-annual-worldwide-infrastructure-security-report-finds-attacker-innovation-and-iot-exploitation-fuel-ddos-attack-landscape.
[59] Roberts, Jeff. "Mobile Security Turns Into Big Business for Cyber Firms." Fortune, January 6, 2017. http://fortune.com/2017/01/06/mobile-cyber-security/.

major stakeholder in determining best strategies to address systemic risk.[60] The preferences of these actors is likely to be diverse as in some places utilities are owned by private actors, in some they are government run, and in some they are owned by actors with close relationships to governing officials.

Public Private Partnership Organizations

While the technology industry has a high interest in protective investment against potential cyber risks, other non-technical industries can also experience large losses in the event of a cybersecurity breach. Since most of this infrastructure is controlled by the private sector, cooperation between government agencies and infrastructure industries is paramount in establishing effective cybersecurity measures. Any major Public Private Partnership organization within a given national space will operate as a stakeholder.

To mitigate cybersecurity risk in the private sector, the government utilizes Public Private Partnerships (PPPs). A PPP is a long-term contract between a government entity and a private enterprise in order to promote a public service where the private enterprise carries significant financial risk. PPPs leverage private resource financing in order to promote infrastructure projects based upon sharing responsibilities and risks involved with operating a public service. Typical responsibilities of the private sector in PPPs include project design, financing, operation, rehabilitation, and maintenance. Essentially, the private sector develops, owns, and operates an infrastructure sector while the government provides incentives without direct funding. For example, PPPs in the transportation sector assist in project risks such as construction, long-term operation and traffic revenue.[61]

However, there are a number of risks involved with PPPs, including projects with existing political or social issues, variances in risk bearing between entities, and reliance on return investment for actors in the private sector. Therefore, a clear regulatory framework is crucial to establishing stable and mutually beneficial PPPS.

PPPs can potentially play a large part in mitigating systemic cyber risk. Cyber PPPs will act by using government resources to monitor and guard networks from any attempted breaches.

---

[60] Douris, Constance. "As Cyber Threats To The Electric Grid Rise, Utilities And Regulators Seek Solutions." Forbes. January 16, 2018. Accessed April 22, 2018. https://www.forbes.com/sites/constancedouris/2018/01/16/as-cyber-threats-to-the-electric-grid-rise-utilities-regulators-seek-solutions/#5477be44343e.

[61] "Public-Private Partnerships." Text. US Department of Transportation, January 23, 2017. https://www.transportation.gov/buildamerica/programs-services/p3

In the event of a cyberattack, the private sector can open communication and further future risk management of cyber threats. However, in order to establish cybersecurity PPPs, issues of data privacy must be addressed. Private industry is reluctant to disclose protected company data and autonomy in their cybersecurity investigations.[62]

Country Actors and Other Organizations

Country representatives, international organizations, and non-governmental organizations (NGOs) are all major stakeholders in cybersecurity systemic stability. Each has its own set of preferences regarding cybersecurity. For countries, preferences are often wrapped up in the type of government and that government's orientation to international Internet Governance. For international organizations, preferences are often related to the objective of the organization. Finally, NGOs interests are also diverse and often are traceable via their missions.

Country Actors

The United Nation's Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) is a good indicator of the major cybersecurity actors that would likely be involved in any cybersecurity regime. The UN GGE was formed in 2004 as a working group to consider the role of international law in the digital space and to begin structuring an international cybersecurity agenda. Since 2004, there have been five UN GGE working groups.

Looking at the 25 members of the 2016-2017 provides insight into the countries that the UN identifies as being likely and capable to play a prominent role in formulating a global cybersecurity agenda and leading an international cyber regime. These include the five UN Security Council Permanent Members—France, the United Kingdom, the Russian Federation, the United States, and China—along with Canada, Mexico, India, Botswana, Brazil, Senegal, Australia, Indonesia, Singapore, Kenya, Egypt, Kazakhstan, Finland, Germany, the Republic of Korea, Serbia, Switzerland, the Netherlands, Estonia, and Cuba.[63] While these countries have wildly disparate interests and beliefs about Internet Governance, they have already collaborated

[62] "A Look into Public Private Partnerships for Cybersecurity." Penn Wharton Public Policy Initiative, April 18, 2017. http://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.
[63] "UN GGE | GIP Digital Watch Observatory for Internet Governance and Digital Policy." Accessed April 29, 2018. https://dig.watch/processes/ungge#Members

in an effort to recognize existing and potential threats, to set expectations of responsible behavior for states, to create measures to build confidence, cooperation, and capacity-building, and to determine how international law applies to the digital space.[64]

International Organizations

International organizations such as the IMF and the World Bank are also significant stakeholders in cybersecurity regimes because of their interest in financial stability and economic growth. The IMF's primary goal is to ensure the stability of the international monetary system, which is a target of cyber threats. As such, the IMF has published working papers to spread awareness and improve understanding of cyber risk, market failures, financial regulation of cyber risk, and methods to improve resilience to cyber risk. The IMF stresses that an effective cyber regulatory regime should undergo continuous evolution to keep pace with new technologies and risks, which requires substantial investment in cybersecurity. Further, the regulatory regime should provide enough structure and supervision to improve security capability and cyber resilience while allowing institutions to retain enough freedom to determine the best methods to address their cyber risks. Additionally, the IMF advocates for collaboration between governments, and recognizes its own role, which it shares with other international organizations, in facilitating such cooperation. This can include resolving disputes, creating coordinated policies, and promoting information sharing.[65] In a future international cyber regime, the IMF could act as a facilitator and intermediary, enabling cooperation and guiding policymaking.

A country that would be a good candidate as a location for future cyber investment would ideally have cyber policies that are in line with what the IMF identifies as best practices. A country that has an established rapport forming or implementing coordinated policies through the IMF would be an especially strong candidate. In the future, structural adjustment programs from the IMF and the World Bank, as well as from other organizations looking to create a more connected world such as the International Telecommunications Union, may require some restructuring of cybersecurity policy because the conditionality of these loans and investments requires governments to adjust economic policies to improve financial stability. A country with

[64] "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law." CCDCOE, August 31, 2015. https://www.ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.
[65] Kopp, Kaffenberger, and Wilson. *Cyber Risk, Market Failures, and Financial Stability.*

well-constructed cybersecurity policies are better able to recognize and mitigate cyber risk, and therefore are more secure candidates for investment.

Non-governmental Organizations

NGOs often seek to form partnerships with governments and businesses to raise awareness of cyber threats and vulnerabilities. They similarly contribute to the improvement of cyber resilience through research aiming to improve security habits and to find solutions to vulnerabilities. While NGOs and advocacy groups typically are not crucial to the functioning of day-to-day cyber resilience, many countries with well-developed cyber policies also have NGOs that help to promote awareness of cyber threats, argue for civil liberties, aid in the settlement of disputes, promote critical infrastructure, and advocate for increased public-private information sharing and partnerships. Some of these NGOs also work directly with governments to accomplish these goals, allowing them to be influential stakeholders in cybersecurity.

The Norwegian Center for Information Security (NorSIS) is an example of a prominent NGO that shares the goals of raising awareness of cyber threats and researching and providing information regarding security habits. In the United States, the TIA Cybersecurity Working Group is a vendor-centric group that advocates for more public-private partnerships, standards for critical infrastructure security, federal funding for cybersecurity research efforts, and improved information sharing from the government to industry regarding cyber intelligence to improve industry effectiveness in preventing and reacting to security threats and incidents.[66] The Cyber Peace Foundation works with several governments and law enforcement agencies to aid in the peaceful settlement of cyber disputes. The Cyber Peace Foundation prioritizes increasing awareness and training for citizens, governments, law enforcement, private companies, and NGOs in order to protect peaceful usage of the Internet and the "conservation of cyber ecosystem."[67] The Anti-Phishing Working Group (APWG) similarly represents an international coalition in support of increasing awareness and cyber research, as well as data exchange and a unified global response to cybercrime.[68]

---

[66] "Cybersecurity | Telecommunications Industry Association." Accessed April 29, 2018. https://www.tiaonline.org/policy/cybersecurity.
[67] "About Us." Cyber Peace Foundation. Accessed April 14, 2018. https://www.cyberpeace.org/about-us.
[68] Baunfire.com, SparkCMS by. "Unifying the Global Response to Cybercrime | APWG." Accessed April 29, 2018. https://www.antiphishing.org//.

While the presence of NGOs or advocacy groups for cybersecurity issues in a given country is not crucial, they do play a role in preventing and addressing cyber risk through promoting information sharing and raising awareness to cyber threats and best practices. They can also highlight potential dangers of technology that private and public stakeholders do not – such as the Electronic Frontier Foundation's work on privacy. Therefore, a country where NGOs or advocacy groups are already active in supporting cyber goals is likely to have a more educated and cautious populace, as well as more active coordination and collaboration regarding cyber policies, threats, and strategy.

Best Practices

Practices that the financial sector uses to mitigate systemic risk that could be transposed into cybersecurity systemic risk mitigation include publishing policy decisions, implementing systemic risk mitigation institutions, filling regulatory gaps, furthering international cooperation, and maintaining global regulatory standards. Across central banks, government agencies, and international organizations, these practices have proved to be useful and can be applied to the field of cybersecurity systemic risk management.

Publishing policy decisions promotes transparency, which is essential in establishing credibility and a positive reputation as an institution. Increasing transparency between the government and companies or individuals could also lessen information asymmetry and alert the public of cyber risk or cyber incidents. Public trust combats contagion in the event of a systemic crisis; accountability lessens an institution's inclination to participate in practices that could pose systemic threats.

The creation of stand-alone systemic risk management entities is also a possibility in developing cybersecurity regulation. Authorities that focus on systemic risk management would further ensure stringent systemic risk policy and fill existing regulatory gaps.

Lastly, fostering a unified international system in mitigating systemic risk could also serve useful to cybersecurity regulators. The financial system is globally interconnected, like the cyber realm. The process of setting global standards for how to manage systemic risk as well as encouraging international cooperation and implementation could be utilized in developing cybersecurity regulation.

References

"2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law." CCDCOE, August 31, 2015. https://www.ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.

"A Look into Public Private Partnerships for Cybersecurity." Penn Wharton Public Policy Initative, April 18, 2017. http://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.

Abomhara, Mohamed, Department of Information and Communication Technology, University of Agder, Norway, Geir M. Kien, and Department of Information and Communication Technology, University of Agder, Norway. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks." *Journal of Cyber Security and Mobility* 4, no. 1 (2015): 65–88. https://doi.org/10.13052/jcsm2245-1439.414.

"About Us." Cyber Peace Foundation. Accessed April 14, 2018. https://www.cyberpeace.org/about-us.

Ahmad, R. A., and M. S. Hashim. "The Organisation of Islamic Conference #x2014; Computer Emergency Response Team(OIC-CERT): Answering Cross Border Cooperation." In *2011 Second Worldwide Cybersecurity Summit (WCS)*, 1–5, 2011.

Allahrakha, Meraj, Paul Glasserman, and H Peyton Young. "Systemic Importance Indicators for 33 U.S. Bank Holding Companies: An Overview of Recent Data," February 12, 2015, 7.

Allen, Bill, Ka Kei Chan, Alistair Milne, and Steve Thomas. "Basel III: Is the Cure Worse than the Disease?" *International Review of Financial Analysis*, Banking and the Economy, 25 (December 1, 2012): 159–66. https://doi.org/10.1016/j.irfa.2012.08.004.

Basel Committee on Banking Supervision, ed. *The G-SIB Assessment Methodology: Score Calculation*. Nov. 2014. Basel: Bank for International Settlements, 2014.

"Basel III: International Regulatory Framework for Banks," December 7, 2017. https://www.bis.org/bcbs/basel3.htm.

Borio, Claudio. "Rediscovering the Macroeconomic Roots of Financial Stability Policy: Journey, Challenges, and a Way Forward." *Annual Review of Financial Economics* 3, no. 1 (December 2011): 87–117. https://doi.org/10.1146/annurev-financial-102710-144819.

Chapman, Ben. "Ireland's Economy Grows 26.3% in 2015 as Corporations Flock to Low Tax Rate | The Independent," July 13, 2016. https://www.independent.co.uk/news/business/news/ireland-s-economy-grows-263-in-2015-as-corporations-flock-to-low-tax-rate-a7133321.html.

"Conference on Operationalizing Systemic Risk Monitoring, May 26–28, 2010 Washington, DC." Accessed April 20, 2018. https://www.imf.org/external/np/seminars/eng/2010/mcm/index.htm.

"Cyber Risk — A Global Systemic Threat", DTCC, October 2014, http://www.dtcc.com/news/2014/october/20/cyber-risk

"Cyber Risk, Market Failures, and Financial Stability." IMF. Accessed April 29, 2018. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104.

"Cyber Security and the Intelligence Community | Belfer Center for Science and International Affairs." Accessed April 29, 2018. https://www.belfercenter.org/publication/cyber-security-and-intelligence-community.

"Cybersecurity | Telecommunications Industry Association." Accessed April 29, 2018. https://www.tiaonline.org/policy/cybersecurity.
"Datacenters.Com: States Competing for Data Centers Extend $1.5B in Tax Breaks," October 5, 2017. https://www.datacenters.com/news/states-competing-for-data-centers-extend-15b-in-tax-breaks.
Dermine, Jean. "Basel III Leverage Ratio Requirement and the Probability of Bank Runs." *Journal of Banking & Finance* 53 (April 1, 2015): 266–77. https://doi.org/10.1016/j.jbankfin.2014.12.007.
Diamant, Aaron. "Ransomware Attack Cost City $2.7 Million, Records Show." *WSB-TV 2*. April 11, 2018. https://www.wsbtv.com/news/local/atlanta/ransomware-attack-cost-city-27-million-records-show/730813530.
Douris, Constance. "As Cyber Threats To The Electric Grid Rise, Utilities And Regulators Seek Solutions." Forbes. January 16, 2018. Accessed April 22, 2018. https://www.forbes.com/sites/constancedouris/2018/01/16/as-cyber-threats-to-the-electric-grid-rise-utilities-regulators-seek-solutions/#5477be44343e.
Du, Brian. "How Useful Is Basel III's Liquidity Coverage Ratio? Evidence From US Bank Holding Companies." *European Financial Management* 23, no. 5 (October 1, 2017): 902–19. https://doi.org/10.1111/eufm.12116.
Elliott, Douglas J. "The Proposed 'Financial Crisis Responsibility Fee.'" *Brookings* (blog), May 11, 2010. https://www.brookings.edu/testimonies/the-proposed-financial-crisis-responsibility-fee/.
"Feds-2018-Ccar.Pdf." Accessed April 29, 2018. https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/feds-2018-ccar.pdf.
Hashim, M. S. b. "Malaysia's National Cyber Security Policy: The Country's Cyber Defence Initiatives." In *2011 Second Worldwide Cybersecurity Summit (WCS)*, 1–7, 2011.
Hill, John. "Using Agent Based Models for Stress Testing." *Simudyne* (blog), February 8, 2018. https://medium.com/simudyne/agent-based-models-for-stress-testing-f8430ed43cdc.
"Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." WIRED. Accessed April 29, 2018. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
"International Country Risk Guide Methodology." The PRS Group. Accessed April 30, 2018. https://www.prsgroup.com/wp-content/uploads/2012/11/icrgmethodology.pdf.
"ISAOs." Cyber Threat Intelligence Network. Accessed April 29, 2018. http://ctin.us/site/isaos/.
"ISPs Treat Cyber Security as a Top Priority." Help Net Security, September 7, 2016. https://www.helpnetsecurity.com/2016/09/07/isps-cyber-security/.
Jogmoo Jay, Choi, and Papaioannou Michael G. "Financial Crisis and Risk Management: Reassessing the Asian Financial Crisis in Light of the American Financial Crisis." *East Asia Law Review* 5, no. 3 (2010): 443–65.
Karisny, Larry. "IoT Is Changing the Cybersecurity Industry." Accessed April 14, 2018. http://www.govtech.com/security/IoT-Is-Changing-the-Cybersecurity-Industry.html.
Kiema, Ilkka, and Esa Jokivuolle. "Does a Leverage Ratio Requirement Increase Bank Stability?" *Journal of Banking & Finance* 39 (February 1, 2014): 240–54. https://doi.org/10.1016/j.jbankfin.2013.11.009.
"Making Derivatives Markets Safer - Financial Stability Board." Accessed April 12, 2018. http://www.fsb.org/what-we-do/policy-development/otc-derivatives/.

"Managing Country Risks: Perspectives for the Post-Crisis Landscape." Oliver Wyman. Accessed April 30, 2018. http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/insights/financial-services/2014/WebsiteUpdates/Managing+Country+Risks%20Update.pdf.

Masciandaro, Donato, and Francesco Passarelli. "Financial Systemic Risk: Taxation or Regulation?" *Journal of Banking & Finance* 37, no. 2 (February 1, 2013): 587–96. https://doi.org/10.1016/j.jbankfin.2012.09.020.

McLymore, Arriana. "Report: Data Centers Are Growing V.A.'s Economy." *AmericanInno* (blog), February 7, 2018. https://www.americaninno.com/dc/inno-news-dc/data-centers-are-bringing-economic-growth-to-northern-virginia/.

Mendelez, Steven. "Police Departments Are Vulnerable To Cyberthreats As Evidence Goes Dig." Accessed April 30, 2018. https://www.fastcompany.com/3055955/police-departments-are-vulnerable-to-cyber-threats-as-evidence-goes-digital.

"Mission & Responsibilities | U.S. COMMODITY FUTURES TRADING COMMISSION." Accessed April 20, 2018. https://www.cftc.gov/About/MissionResponsibilities/index.htm.

Narayan, Sethi, Sahoo Kalpana, and Sucharita Sanhita. "A SURVEY OF INTERNATIONAL FINANCIAL RISK MANAGEMENT SYSTEM." *Journal of Public Administration, Finance and Law*, no. 4 (2013): 186–203.

National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0." Gaithersburg, MD: National Institute of Standards and Technology, February 12, 2014. https://doi.org/10.6028/NIST.CSWP.02122014.

NATO, "NATO Cyber Defence Factsheet", February 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf

OECD. *Systemic Financial Risk*. OECD Reviews of Risk Management Policies. OECD Publishing, 2012. https://doi.org/10.1787/9789264167711-en.

Perotti, Enrico. *Tax Banks to Discourage Systemic-Risk Creation, Not to Fund Bailouts*. London: CEPR Press, 2010. http://www.voxeu.org/content/post-crisis-banking-regulation-evolution-economic-thinking-it-happened-vox.

Persaud, Naresh. "2018 Prediction: Securing IoT-Connected Devices Will Be a Major Cybersecurity Challenge." CSO Online, December 22, 2017. https://www.csoonline.com/article/3244467/internet-of-things/2018-prediction-securing-iot-connected-devices-will-be-a-major-cybersecurity-challenge.html.

"Perspectives on CCAR.Pdf." Accessed April 29, 2018. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Perspectives%20on%20CCAR%20Confronting%20uncertainty%20in%20the%202018%20cycle/Perspectives%20on%20CCAR.ashx.

Peter, Moles. "Financial Risk Management: Sources of Financial Risk and Risk Assessment." Course Text. Edinburgh Business School: Heriot-Watt University, 2016. https://www.ebsglobal.net/EBS/media/EBS/PDFs/Financial-Risk-Management-Course-Taster.pdf.

Peter Sommer, and Ian Brown. *Future Global Shocks*. OECD Reviews of Risk Management Policies. OECD Publishing, 2011. https://doi.org/10.1787/9789264114586-en.

Pickett, Christopher J. "An Agent-Based Network Simulation Model for Comprehensive Stress Testing and Understanding Systemic Risk." *College of William & Mary Undergraduate Honors Theses*, April 2014, 45.

Poledna, Sebastian, Olaf Bochmann, and Stefan Thurner. "Basel III Capital Surcharges for G-SIBs Are Far Less Effective in Managing Systemic Risk in Comparison to Network-Based, Systemic Risk-Dependent Financial Transaction Taxes." *Journal of Economic Dynamics and Control* 77 (April 1, 2017): 230–46. https://doi.org/10.1016/j.jedc.2017.02.004.

Police Executive Research Forum. "The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime.," 2014. http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf.

Pozsar, Zoltan, Tobias Adrian, Adam Ashcraft, and Hayley Boesky. "Federal Reserve Bank of New York Staff Reports," n.d., 82.

"Presidential Policy Directive -- Critical Infrastructure Security and Resilience." whitehouse.gov, February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

PricewaterhouseCoopers, "System and Organization Controls (SOC) Reporting," PwC, accessed May 10, 2018, https://www.pwc.com/us/en/services/risk-assurance/third-party-assurance/soc-reporting.html

"Public-Private Partnerships." Text. US Department of Transportation, January 23, 2017. https://www.transportation.gov/buildamerica/programs-services/p3.

"Reducing Systemic Risk in the Financial Sector." Accessed April 20, 2018. https://www.brookings.edu/testimonies/reducing-systemic-risk-in-the-financial-sector/.

Report, Security. "Arbor Networks' 12th Annual Worldwide Infrastructure Security Report." Arbor Networks®, January 24, 2017. https://www.arbornetworks.com/arbor-networks-12th-annual-worldwide-infrastructure-security-report-finds-attacker-innovation-and-iot-exploitation-fuel-ddos-attack-landscape.

Roberts, Jeff. "Mobile Security Turns Into Big Business for Cyber Firms." Fortune, January 6, 2017. http://fortune.com/2017/01/06/mobile-cyber-security/.

"SEC.Gov | About the SEC." Accessed April 29, 2018. https://www.sec.gov/about.shtml.

"SEC.Gov | Striving to Restructure Money Markets Funds to Address Potential Systemic Risk." Accessed April 30, 2018. https://www.sec.gov/news/public-statement/2013-06-05-open-meeting-statement-laa.

Siegel Bernard, Tara, and Stacy Cowley. "Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says." *The New York Times*. October 3, 2017. https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html.

Skierka, Isabel, Robert Morgus, Mirko Hohmann, and Tim Maurer. "CSIRT Basics for Policy-Makers," n.d., 28.

Stijn, Claessens, and Kose M. Ayhan. "Financial Crises: Explanations, Types, and Implications." International Monetary Fund, n.d. https://www.imf.org/external/pubs/ft/wp/2013/wp1328.pdf.

"Take Cybersecurity Away From Spies - For Everyone's Sake." Chatham House. Accessed April 29, 2018. https://www.chathamhouse.org//node/31614.

The Economist. “Crisis Mismanagement.” *The Economist*, October 27, 2012. https://www.economist.com/news/books-and-arts/21565142-how-america-bailed-out-banks-rather-its-citizens-crisis-mismanagement.
“The Fed - Challenges Associated with Using Rules to Make Monetary Policy.” Accessed April 13, 2018. https://www.federalreserve.gov/monetarypolicy/challenges-associated-with-using-rules-to-make-monetary-policy.htm.
“The Fed - Stress Tests and Capital Planning.” Board of Governors of the Federal Reserve System. Accessed April 29, 2018. https://www.federalreserve.gov/supervisionreg/stress-tests-capital-planning.htm.
“The Military Role in National Cybersecurity Governance.” *Brookings* (blog), November 30, 2001. https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/.
The Office of Financial Research, “Cybersecurity and Financial Stability: Risks and Resilience,” February 15, 2017, 12.
“Transparency International - What Is Corruption?” Accessed April 22, 2018. https://www.transparency.org/what-is-corruption#costs-of-corruption.
“UN GGE | GIP Digital Watch Observatory for Internet Governance and Digital Policy.” Accessed April 29, 2018. https://dig.watch/processes/ungge#Members.
“Unifying the Global Response to Cybercrime | APWG.” Accessed April 29, 2018. https://www.antiphishing.org//.
Wallace, Ian. “The Military Role in National Cybersecurity Governance.” *Brookings* (blog), November 30, 2001. https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/.
Williams, Katie Bo “G20 Nations Reach Anti-Hacking Pledge,” Text, The Hill, November 17, 2015, http://thehill.com/policy/cybersecurity/260414-g20-nations-reach-anti-hacking-pledge
Woo, Venetia, Bharat Chelluboina, and Wilfrid Xoual. “The Effectiveness of the Regulatory Stress Testing Disclosure Process.” *Financial Markets, Institutions & Instruments* 23, no. 1 (February 1, 2014): 1–70. https://doi.org/10.1111/fmii.12014.
World Economic Forum. “How Can We Control Systemic Risk? | World Economic Forum,” August 10, 2015. https://www.weforum.org/agenda/2015/08/how-can-we-control-systemic-risk/.
Wright, Morgan. “A Ransomware Attack Brought Atlanta to Its Knees — and No One Seems to Care.” *The Hill*. April 4, 2018. http://thehill.com/opinion/cybersecurity/381594-a-ransomware-attack-brought-atlanta-to-its-knees-and-no-one-seems-to.

Team Bios

Faculty Lead

Jessica Beyer (jlbeyer@uw.edu): Jessica Beyer is a Lecturer and Research Scientist in the Henry M. Jackson School for International Studies. Her current research focuses on cybersecurity issues, particularly non-state actors and international security. Her past research explored political mobilization emerging from highly populated online communities and focused on actors such as Anonymous and other hacktivists, the Pirate Parties, and digital pirates. In 2012, she won the Association of Internet Researcher's Dissertation Award. Her book, *Expect Us: Online Communities and Political Mobilization*, was published by Oxford University Press in 2014. Jessica holds her Ph.D. in Political Science from the University of Washington.

ARP Program Manager

Allison Anderson (allyja@uw.edu): Allison Anderson is a Ph.D. student at the Jackson School of International Studies. Her research interests are centered around gender, development, and information and communications technologies (ICTs) in the Arab world. She is currently studying pathways to women's economic participation in Jordan. Allison came to the Jackson School from the Bill and Melinda Gates Foundation, where she focused on strategic planning and engagement in the Office of the President for Global Health. Previously, she worked at Deloitte Consulting conducting political risk analysis and market research for both public and private sector clients. Allison served two years in the U.S. Peace Corps in Jordan. Allison received her M.A. from Johns Hopkins Paul H. Nitze School of Advanced International Studies (SAIS) where she focused on Strategic Studies and International Economics. She holds a B.A. in Political Science and Arabic & Islamic Studies from the University of Michigan.

Senior Research Fellow

Alex Wirth (awirth2@uw.edu): Alex Wirth is senior at the University of Washington with an intended major in International Relations from the Jackson School of International Studies with a minor in Human Rights Studies. With a special interest in the impact of international politics on development, security, and the economy, Alex has worked during college as an intern for the United States Department of State and as a Strategic Intelligence Research Fellow for Microsoft. Beyond international relations, Alex is also passionate about higher education policy, particularly in the state of Washington, and has served as the Director of Government Relations for the Associated Students of the University of Washington. Alex also currently serves on the editorial board of the Jackson School Journal of International Studies, and as editor for the 2018 Jackson School taskforce on election interference. Outside of school, Alex is an aspiring decent chef, a music nerd, a fan of kayaking, and an avid geocacher (please ask!).

Research Fellows

Conor Cunningham (ccc12@uw.edu): Conor Cunningham is currently a senior studying International Studies with a focus on foreign policy, diplomacy and security. He is currently pursuing a minor in Russian language and acquired advanced proficiency in French after living in Switzerland in middle school. He is interested in Eastern Europe, specifically regarding issues of nationalism, security, and religion. He has committed to studying abroad in Moscow over the summer of 2018 in an intensive Russian language program. He was also recently notified that he

is a recipient of the Foreign Language Area Fellowship for Russian for the 2018-2019 school year.

Cynthia Hannon (hannoc@uw.edu): Cynthia Hannon is an International Policy Institute Research Fellow. She is a recent graduate of the Henry M. Jackson School of International Studies, where she earned a B.A. in International Studies with an emphasis on political economy. Her regional specialty is East Asia, namely the trilateral relationship between the United States, Japan, and China. Cynthia recently led a Task Force in Winter 2018 regarding the impact of populism on democratic institutions.

Mariam Malik (mariam06@uw.edu): Mariam Malik is an International Policy Institute Research Fellow. Currently a senior studying Human Rights and the Law at the Jackson School of International Studies, she was a part of the 2018 Task Force, "NATO and Russia: Strengthening the Alliance and Improving Resilience" in Rome, Italy, focusing on the use of information in hybrid warfare and Cybersecurity. Born and raised in Karachi, Pakistan, she is also majoring in Comparative Literature: Cinema and Media Studies and is fluent in three languages.

Rachel Paik (racpaik@uw.edu) Rachel Paik is a senior at the Jackson School and is set to graduate this spring 2018 with a B.A. in International Studies and a minor in Korea Studies. Her research interests include: nuclear security, US- ROK relations, and US prison reform. In addition to participating in the Spring 2018 Microsoft Applied Research Project as an IPI research fellow, she is also the recipient of the FLAS fellowship from the East Asia center and was selected to participate in the Slade Gorton Global Leaders Program hosted by the National Bureau of Asian Research. She was most recently the coordinator of the Winter 2017-2018 task force addressing the North Korean Nuclear Crisis and is continuing to pursue research in nuclear studies as a 2017-2018 NEREC Young Fellow at KAIST University in Daejeon, South Korea.

Rishi Paramesh (riparam@uw.edu): Rishi Paramesh is an International Policy Institute Fellow for Microsoft's Global Security Strategy & Diplomacy Project. He is currently a junior at the University of Washington, majoring in Foreign Policy and Diplomacy through the Henry M. Jackson School of International Studies and International Security through the Political Science Department. Rishi was a member of the Winter 2018 Rome Task Force, "NATO and Russia: Improving Resistance and Strengthening the Alliance." In his free time, Rishi enjoys traveling, learning about culture and language, and cooking.

Heidi Samford (hjs54@uw.edu): Heidi Samford is a senior graduating from the Henry Jackson School of International Studies in 2018 with a focus in Foreign Policy, Security, and Diplomacy. She was a member of the Winter 2018 Task Force, "Hacking Democracy: Cybersecurity and Global Election Interference." Her current research interests include cyberwarfare, information security, arms control, and the Middle East.

Kunat Sangcharoenvanakul (kunats@uw.edu): Kunat Sangcharoenvanakul is an International Policy Institute research fellow. Currently, he is a senior pursuing a B.A. in International Studies with an emphasis on international political economy at the Henry M. Jackson School of International Studies. Kunat was a member of the Winter 2018 Task Force on the Future of US

Foreign Aid: Comparisons and Recommendations. His research interests are in the field of political economy, international trade and development, and Southeast Asia. In addition to his research interests, he had recently interned at PricewaterhouseCoopers as a consultant for customs and international trade.

Sarah Sanguinet (sasangui@uw.edu): Sarah Sanguinet is an International Policy Institute Research Fellow for the Microsoft Applied Research Project of Spring 2018. She will be working with Microsoft's Global Security Strategy & Diplomacy team, focusing on potential systemic risk in cybersecurity. She is a junior at the University of Washington, studying International Political Economy within the Henry M. Jackson School of International Studies. Sarah's research interests include global health strategy, digital diplomacy and cybersecurity policy.

Alison Wattles (awattles@uw.edu): Alison Wattles is a masters student in the University of Washington's Henry M. Jackson School of International Studies. She is also a UW graduate, having earned her BA in European Studies and French in 2015. Before returning for her MA, she spent a year teaching French at a local high school. She is most interested in security and conflict resolution, and her current research focuses on trends of Islamist radicalization in France.

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON

The Henry M. Jackson School of International Studies
jsis.washington.edu