Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

United States–China Collaboration on the Internet of Things Safety:

WHAT NEXT?

Karl Frederick Rauscher

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

United States–China Collaboration on the Internet of Things Safety:

WHAT NEXT?

Karl Frederick Rauscher

ISBN: 978-1-61977-079-9

December 2019

Preface

At the time of this report's writing, the United States and China are engaged in intense trade negotiations. Central to this "trade war" is how the two countries will protect their interests in emerging technologies—technologies that can have a decisive role in their respective national security and economic prosperity. The outcome of these negotiations is anticipated to be nothing less than a watershed for the future of the US-China relationship, and also for the rest of the world. On one hand, the final disposition may result in a decoupling of the two largest economies in history—something both sides indicated a willingness to accept. On the other hand, the outcome may be more vigorous trade than occurred before. For either of these dispositions, as well as for hybrids, it is clear that there are uncertainties that must be faced—none more important than how the two countries will engage around emerging technologies, such as the Internet of Things (IoT).

IoT is poised to be a tsunami of transformation for every industry sector. IoT is the overarching vision for 5G mobile networks, artificial intelligence (AI), and the interconnection of myriad devices. IoT offers many benefits for the prosperity and well-being of citizens of both countries, and the rest of the world. As with previous major technology advances, there are also great fortunes to be made. However, the pervasive nature of IoT has many concerned with potential impacts on the safety and security of societies everywhere.

Like cybersecurity, IoT safety and security must be a team effort; i.e., both countries need the help of industry subject-matter experts and business leaders to prepare for the future. However, just how the United States and China will interact with each other will remain complicated for some time. US and Chinese entrepreneurs have forged complementary business relationships that have served both countries, and the rest of the world, throughout the recent Internet revolution. Despite these past successes, there arise bigger issues concerning emerging technologies. Preparing for the IoT transformation offers both the United States and China opportunities to consider limited endeavors to cooperate in addressing unresolved issues that affect both countries.

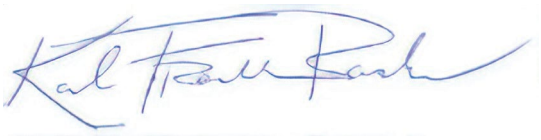
This report presents four recommendations for the governments of the United States and China to decisively reduce the risks that both countries face as a result of the quickening adoption of the Internet of Things. The recommendations simultaneously address risks to national security, open new doors to commercial enterprise, and protect the interests of the general public. Given the criticality of expanding national dependence on IoT, and the growing consequences of IoT failures, this report urges senior government leaders in both countries to study and implement these recommendations with urgency commensurate with the stakes at play.

Given that IoT and related technologies, such as 5G and AI, are first and foremost scientific and engineering disciplines, it is vital that governments effectively engage experts for support in addressing these concerns and implementing the recommendations.

IoT is big; it is poised to cast a shadow on every industrial transformation that has preceded it. However, as is often the case, the rapid advances in technology have outpaced corresponding policy, leaving an ever-growing gap as the advances continue. This gap results in a sub-optimal environment for the technology to develop and be deployed, and thus for stakeholders—such as business enterprises and consumers—to benefit. Action from government and business leaders is imperative.

For those who are not avid followers of high-tech advances, the content in the following pages may read like science fiction. Let me assure you, I have never been that interested in fanciful genres; I simply find reality far more interesting, and more valuable to spend time thinking about. To borrow a phrase from C.S. Lewis, however, I am a "reluctant convert." Like you, I am witness to the autonomous vehicles and virtual assistants that have entered our world. But, this is just the beginning. We can now see the missing pieces to a grand puzzle being solved with 5G, AI, and robotics. Step by step, we are getting closer to what used to be called science fiction. The next decade or two should be fascinating. It will be much better for all of us if we get this right.

Finally, thank you to the individuals on the next page for their contributions to this effort.



Karl Frederick Rauscher

Acknowledgments

The staff of the China Institutes of Contemporary International Relations and Atlantic Council for their participation in capturing insights from the bilateral workshop that launched this effort, including Josh Corman, Beau Woods, and Klara Tothova Jordan for their leadership and vision.

Stuart Goldman, Richard Krock, Dan O'Neill, and Konrad Rauscher for their expertise, research, and edits.

Barry Pavel for his courage in extending the scope of the Atlantic Council's Scowcroft Center for Strategy and Security.

James Seng for his insights on Chinese and US technology and policy trends.

C.H. Tung and the China-United States Exchange Foundation for their long-term support in exploring new opportunities to better China-US relationships.

Contents

List of Figures

"The future ain't what it used to be."

YOGI BERRA

Executive Summary

During the preparation of this report, historic trade negotiations were under way between the United States and China. Because advanced technologies have been central to this "trade war," it is all but certain that the previous dispensation will be eclipsed by a new structure and new rules for how emerging technology will be addressed. Whatever the outcome, scientific and engineering breakthroughs on the horizon are evoking important questions: How can each country protect its national security interests? Will each country have a role in each other's markets? Are there limited areas of cooperation in which even the most competitive and mistrusting of countries can work together?

The Internet of Things is the term adopted to describe a future world with pervasive connectivity. The curious, formal use of the word "things" admits that all the implications of where things are headed are not fully understood—exactly what will be connected with what?

The vision for the future scope of the Internet is colossal. The size of the future Internet can be understood from its addressing scheme, which allows for undecillion unique addresses—trillions times trillions times trillions. Imagine any important "thing" being connected to the Internet.

In many regards, this future has already arrived. People now have connected homes with networked light bulbs, doorbells, security cameras, and refrigerators, while time away from home increasingly involves interconnection with online cars, trains, and airplanes. The very foundations of sustenance are on their way to being networked, with soil-moisture sensors, insect- and disease-inspecting aerial drones, and real-time tracking of supply chains. Even human bodies are being brought online, with vital-sign monitoring, and nanotechnology will soon inhabit their bloodstreams. The ultimate "thing" to connect to the Internet, however, will be humanoid robots—human-like machines that increasingly operate among the real thing.

Artificial intelligence, robotics, and the introduction of 5G mobile networks are technologies that, on their own, promise to ignite explosive wealth creation and spark exponential growth in economic development. The intersection of these three technologies, however, is expected to serve as a catalyst for innovation that will transform society more than any technology advances to date, including the Internet. Indeed, breakthroughs in AI, robotics, and the deployment of 5G mobile networks make possible "cloud robotics"—many humanoid robots connected to shared brains that are continuously learning, each operating seamlessly in peoples' midst, performing the tasks that people prefer not to do, and utilizing skills that humans don't have.

IoT promises to transform quality of life to an extent that is difficult to imagine. The commercial opportunities associated with these technologies will likely create hundreds of new multi-billion- dollar companies. The persuasive power that the economic benefits of IoT portend may be overwhelming for conventional approaches to national security. For economic and practical reasons, it is unwise to impede the advance of such powerful technologies. Yet, how will nation-state security interests be protected? Can a nation state afford to fall behind the pace of IoT adoption? What advantages will those leading research and development have? Are existing frameworks sufficient for managing the challenges of IoT security?

This report argues that a great disservice to stakeholders is done: when IoT technology is insufficiently understood; when national security, commercial, and humanitarian interests are conflated; and when opportunities for cooperation are dismissed out of hand.

The world's two largest powers—the United States and China—are at a crossroads with regard to their level and scope of cooperation in continued IoT advances. Both the potential risks and potential benefits from cooperation are enormous in the areas of commercial and humanitarian interests. Though the United States and China have a long history of cooperation, and the two countries have never directly engaged as adversaries in a war, the relationship is at an impasse regarding how

competition will play out going forward. At a basic level, the rise of China introduces chaos to the world order that the United States has maintained for decades. Adding IoT to the mix will further upend the existing world, but paradigm shifts are nothing new. How can the United States and China test the waters? Are there limited areas of cooperation that merit being confronted together, to reduce the unknowns and dangers that will be unleashed by the impending IoT tsunami?

For IoT, the answers to these questions must meet the challenges of **protecting national security interests, while not significantly hampering innovation and business development**.

If the trends described above are even slightly true, ignoring them is irresponsible. Stopping technology is neither possible nor economically desirable, and is an overreaction doomed from the start. The alternative is addressing the challenges that IoT advances will present. Can the United States and China work together, with some limited scope, to establish consensus on policies and standards to make their societies safer and provide a model for the world? Could such cooperation, once manifested, spark the broader international cooperation needed for IoT safety?

This report answers these questions by offering four recommendations. The recommendations are introduced here in brief, and presented fully in Section 4.

Recommendation No. 1
Distinct Policies for National Security, Commercial, and Humanitarian Interests in IoT
The United States and Chinese governments should distinguish between national security, commercial, and humanitarian interests in establishing policies for the Internet of Things.

1 The first recommendation begins with the observation that IoT is analogous to the wheel—an innovation used for a variety of purposes, including national security, commercial, and humanitarian ones. As a wheel can be used as an integral part of the landing gear of a stealth bomber, the local pizza-delivery fleet, or an ambulance, IoT concepts and technologies are used to network battlefield assets, track supply-chain inventory in real time, and extend advanced healthcare via outpatient medical devices. Policies that fail to come to grips with the distinct interests and pervasive applications of IoT (and related technologies such as AI) can be crippling to national security, economic development, and human welfare.

Presently, discussions around IoT often conflate the interests of national security, commerce, and the general public's welfare. This thinking is problematic, in that it hinders fully effective engagement with any one of these interests, as well as the optimization of these domains as a whole.

The first recommendation directs decision-makers to establish policies that allow for the optimization of IoT in a manner beneficial for each of these three areas.

Supporting material for decision-makers is outlined in Section 4.1 for this recommendation. Supporting material for this and all subsequent recommendations includes the required commitments, alternatives and consequences, benefits of implementation, next steps, and measures of success.

This first recommendation is foundational to the remaining three recommendations, which each separately advance limited US-China cooperation for national security, humanitarian, and commercial interests.

Recommendation No. 2
Priority Scheme for Critical Human and Machine Communications
The US government and Chinese government should agree on a priority scheme for communications traffic across the Internet of Things, to ensure critical US-China communications for both humans and machines during a crisis.

2 The second recommendation addresses one of the most glaring challenges of IoT for the future: network congestion. It is worth noting that the realities of this concern have already been experienced via denial-of-service (DoS) attacks, in which many IoT devices have been orchestrated for harmful purposes. IoT is a catalyst for a number of changes, but one fact that does not change is that tomorrow's networks, like today's, will have capacity limitations. Networks are not designed nor built to handle 100 percent of the potential traffic end devices can generate. Building such capacity levels is undesirable, as it would increase the cost of services by an order of magnitude or more. However, IoT uniquely exacerbates

the intrinsic vulnerability of all networks to have capacity limitations. A malicious actor is not even needed to cause problems.

IoT combines several difficult factors: an exponentially increased number of connected devices, devices that will have extremely high bandwidth needs, and uncoordinated bandwidth utilization. When these factors are combined, it is a straightforward conclusion that congestion will be much more frequent even without a malicious actor. This congestion results in blocked transmissions (e.g., phone calls, messaging, machine-to-machine communications). The national security interests of both the United States and China could be negatively impacted if critical US-China communications between humans and machines were impaired during a crisis.

Supporting material for decision-makers is outlined in Section 4.2 for this recommendation.

Recommendation No. 3

Extend the Envelope for Humanitarian Collaboration

The US government and Chinese government should cooperate on humanitarian applications of the Internet of Things by stating respective policies, providing feedback on the acceptability of each other's policies, collaborating on investigations when incidents appear noncompliant with stated policies, and confronting parties responsible for causing harm to human-welfare interests in the Internet of Things.

3 The third recommendation identifies limited opportunities to collaborate where there are no complications with national security or commercial competitiveness. There are problems, for example, in the healthcare arena, where the benefits of collaboration will benefit citizens of both the United States and China, as well as people in other countries.

IoT has great potential for improving the lives of families. Indeed, the healthcare sector is one of the anticipated early adopters of IoT. With aging populations, the demand for quality healthcare is a major concern for both the United States and China. The trends of growing needs and ever-higher expectations, combined with the realities of a limited number of healthcare professionals and limited budgets, set the stage for a collision of hopes and reality. IoT cannot arrive soon enough for the healthcare sector. One potential application is the monitoring of a health crisis in real time, a situation for which IoT and AI are well suited to help. Such collaboration would further extend the lessons learned from the cooperation in response to the 2002 severe acute respiratory syndrome (SARS) epidemic.

Given past formal agreements on international humanitarian law, it is reasonable to suggest that both countries can initially cooperate on human-welfare applications of IoT, at least on a limited basis. There are three important stages where specific cooperation would be helpful: common ground for what should be protected, a process for how apparent exceptions can be reviewed, and the criteria for when a joint response should be made against offenders. Cooperation in these stages, even for a narrow scope, will provide opportunities for trust building and further cooperation across a broader scope of humanitarian interests.

This recommendation emphasizes the upside opportunities IoT provides the United States and China for new cooperation that can benefit both citizenries, as well as the rest of the world.

Supporting material for decision-makers is outlined in Section 4.3 for this recommendation.

Recommendation No. 4

Unleash Entrepreneurs with Verifiable Acceptable Practices

The US and Chinese governments should, in proportion to the degree each is resolved to encourage the development of a thriving Internet of Things business environment in their respective economies, unleash entrepreneurs by: ensuring fair trade for businesses with IoT products and services; defining the specific acceptable criteria for any trustworthiness requirements for products or services; and providing opportunities for products and services to be verified against the same criteria in an objective process.

4 Both the United States and China, as well as many other nation states, see IoT and related technologies as key to economic growth in the coming decade. Both countries would like their businesses to have access to each other's enormous markets, and both would like their businesses to be major players internationally. The opportunities for

wealth creation are unprecedented. From an entrepreneur's perspective, the emerging IoT landscape is full of opportunities.

However, entrepreneurs face a major challenge from the risk of uncertain regulatory measures, which may include restrictions on such things as investments, sales, component integration, and mergers and acquisitions. Though well intentioned, these regulations are typically problematic for businesses, and are often vague regarding what is actually required to be acceptable. This lack of specificity is based on the commonly held attitude that the technology is too complex and the actual problems are not known. Instead of a knowledge of the intrinsic vulnerabilities within the technology that could be exercised by threats, mere historical analogy is often used as the primary basis of informing and establishing priorities and the language of policies.

This recommendation emphasizes the priorities of businesses, and specifically those enterprises most likely to take risks to create new wealth across the emerging IoT landscape. The recommendation recognizes that the deployment of IoT exposes national critical infrastructure to increased risks and, thus, is a national security concern. Indeed, the worst-case scenarios regarding IoT are real possibilities, and a wide range of scenarios could foreseeably involve loss of life and property on a large scale. There is no doubt that governments need to be cautious about the role that foreign businesses are allowed to have within their respective realms.

Fear of worst-case scenarios will not arrest the deployment of IoT, as its benefits—unprecedented economic and humanitarian advances, including enhancements to critical-infrastructure efficiency and reliability—are too compelling. The responsible way to address these real concerns is with appropriate due diligence.

The following recommendation seeks to seize the economic opportunity IoT presents, while respecting the daunting security concerns involved. The recommendation appropriately engages IoT, in that it forces the discussion at the level of accountability—both for businesses and regulators. The recommendation is actionable, in that all of the required commitments are reasonable and preserve self-interest. The recommendation is bold, in that it replaces the status quo bureaucracy with informed, surgical methods.

Supporting material for decision-makers is outlined in Section 4.4.

The report's introduction (Section 2) describes the approach taken in its preparation, along with the scope and motivation for this initiative. The report presents eighty-three key observations (Section 3) that are critical to understanding both the IoT challenges and the attributes of the solution space for promoting personal safety and national security. The report moves next to outline the findings of a systematic analysis (Appendix A, Application of the Eight-Ingredient Framework to the Internet of Things) of the scientific principles and engineering practices that underpin IoT. Finally, these observations and findings are used to define the solutions space and forge practical, actionable recommendations (Section 4), which, if implemented, will promote nation-state security interests, as well as protect the safety interests of their citizens.

Once the dust settles on the current trade negotiations, the United States and China will be faced with how to deal with the emerging IoT transformation. Whatever the outcome, it seems certain that the US-China relationship will remain complicated. In light of respect for both this complexity and the unfolding IoT challenges, the reader is encouraged to consider these recommendations, study the underlying support for each, and join the effort to enhance limited, responsible cooperation between the United States and China with the aim of helping the IoT make tomorrow more prosperous, safer, and more secure.

"One generation plants trees and another gets shade."

ANCIENT CHINESE PROVERB

2. Introduction

This report explores the potential for limited collaboration between the United States and China with regard to IoT, once clarity is provided from the contemporaneous trade negotiations. This subject resides at the nexus of three highly complex areas: rapidly advancing, radical technology; highly competitive business involving the two largest economies in history; and international relations between superpowers. The stakes are high for both countries, as well as for the rest of the world.

This report is not an academic exercise. On the contrary, this document has been prepared to address the problem head on, presenting actionable recommendations for top-level decision-makers, which, if implemented, would significantly reduce the exposure of both the United States and China to the very real risks that IoT poses to public safety and security. Their implementation would, moreover, promote a thriving IoT marketplace and nurture a wide array of humanitarian benefits from the emerging technology.

Given the significance of this undertaking, this section offers a review of the fundamental parameters that have formed the recommendations. It answers three basic questions. Why produce this report? What is the scope of the report? How was the report prepared?

2.1 MOTIVATION FOR THIS REPORT

Why produce this report?

This report is needed because the opportunities and consequences of IoT are profound, and the process leading to any policy that can affect the ability to take opportunities and manage consequences requires due diligence in both completeness and rigor. Further to this point, this report is necessary because existing policy discussions about IoT lack a sufficient and comprehensive mastery of the far-reaching impacts of IoT technology.

China and the United States are the world's two biggest cyber powers, and simultaneously have both common and competing interests when it comes to IoT. Both policies that fail to effectively address competing interests and policies that miss opportunities for cooperation can have unacceptable, dire consequences for both the United States and China.

Prior to the September 11, 2001, terrorist attacks, established White House national security policy considered the nation's energy infrastructure the most critical among all of the national critical infrastructures (transportation, water, healthcare, etc.). However, in the aftermath of that historic crisis, the status of "most critical" among the critical infrastructures was updated to include the communications infrastructure. This change was the result of the simple recognition that every other critical infrastructure relies upon energy and communications. The energy and communications infrastructures were, therefore, central to critical-infrastructure protection. This was a lesson learned. Today, and for the foreseeable future, the central role of the communications infrastructure is greatly expanding, as is the reliance upon it. IoT is the reason. IoT is poised to connect any thing that is, or can become, important. Thus, critical-infrastructure protection—and, therefore, national security—is inseparably intertwined with IoT going forward. Furthermore, an appreciation for the pervasive connectivity of IoT, and its increasingly impactful role in autonomous processes, must be a central part of protecting the communication infrastructure—and, thus, all national critical infrastructures—going forward.

While IoT is important to critical-infrastructure protection, and to national security more broadly, much—if not most—of IoT will not have critical national security implications; i.e., it will be used primarily for commercial and humanitarian applications.

China has the largest communications infrastructure in the world, serving more than eight hundred million netizens. China's economic growth depends on its critical infrastructures, as well as the continued adoption of technologies such as IoT. As a leading manufacturer,

China is also a major provider of IoT products for the United States and the rest of the world. These products include both peripheral devices (i.e., "things") and core infrastructure for communications networks. Thus, the subject of China is, fittingly, a part of any discussion on this subject matter for US stakeholders.

Obviously, the United States and China are not alone in their adoption of IoT, nor in their plans for more technologically advanced societies. Thus, the report's analysis and recommendations also consider the implication of US and Chinese policies for the broader international marketplace and nation-state stakeholders.

2.2 SCOPE OF THIS REPORT

What is the scope of this report?

The scope of this report is understanding the potential range for the US-China relationship regarding IoT safety. This report's scope covers a broad set of interests for both countries, namely national security, commercial, and humanitarian interests.

Benefits

NATIONAL SECURITY INTERESTS: primarily concerned with the protection of citizens, economy and institutions.

COMMERCIAL INTERESTS: primarily concerned with creating wealth or making financial profits.

HUMANITARIAN INTERESTS: primarily concerned with seeking or promoting human welfare.

Regarding the technology aspect of this undertaking, the report scope covers the IoT and the system of connected entities that exchange, transmit to, and/or receive information from other connected entities. The entities could be literally any thing. The scope includes the current state of IoT implementation, as well as future states now under development that extend IoT to ever more sophisticated applications. Many underlying technologies support IoT, including, at a high level: any type of computer processor; software, including AI; passive sensors, smart machines, and robots; proprietary and open protocols; and existing wireline and wireless networking standards; as well as emerging 5G and beyond.

Also included in the scope of this report is understanding "best-case" and "worst-case" scenarios. These extremes are used as reference points to assess the acceptability of risks and feasibility of solutions.

2.3 METHODOLOGY OF THIS REPORT

How was the report prepared?

The methodology used to produce this report consisted of four stages: information gathering, systematic analysis, problem solving, and report generation and outreach.

Information Gathering

During the first stage of information gathering, a workshop was held in which members of the Atlantic Council's Scowcroft Center engaged with members of the China Institute of Contemporary International Relations (CICIR). The workshop was hosted by CICIR in Beijing during the summer of 2018. The objective of the workshop was to open a dialogue about possible areas of cooperation between the United States and China regarding IoT safety.

Additional research was conducted on the nexus of IoT technology, business trends, and the US-China relationship. This first stage culminated with the identification of factors that can have a decisive impact on the interfaces within the nexus. Eighty-three key observations have been captured, and are included in Section 3.

Figure 1. Eight-Ingredient (8i) Framework

Systematic Analysis

The second stage involved an in-depth, systematic analysis of the key observations in light of the intrinsic vulnerabilities of cyberspace. Given that IoT is primarily a scientific and engineering arena, such an approach is necessary to perform due diligence for the subject matter. The objective of this analysis was to use a comprehensive approach to identify which attributes of IoT would make cyberspace more likely to be exploited. Much of this analysis is more detailed and technical than the audience is likely to find accessible, so Appendix A, Application of the Eight-Ingredient Framework to the Internet of Things, presents a high-level summary of the approach.

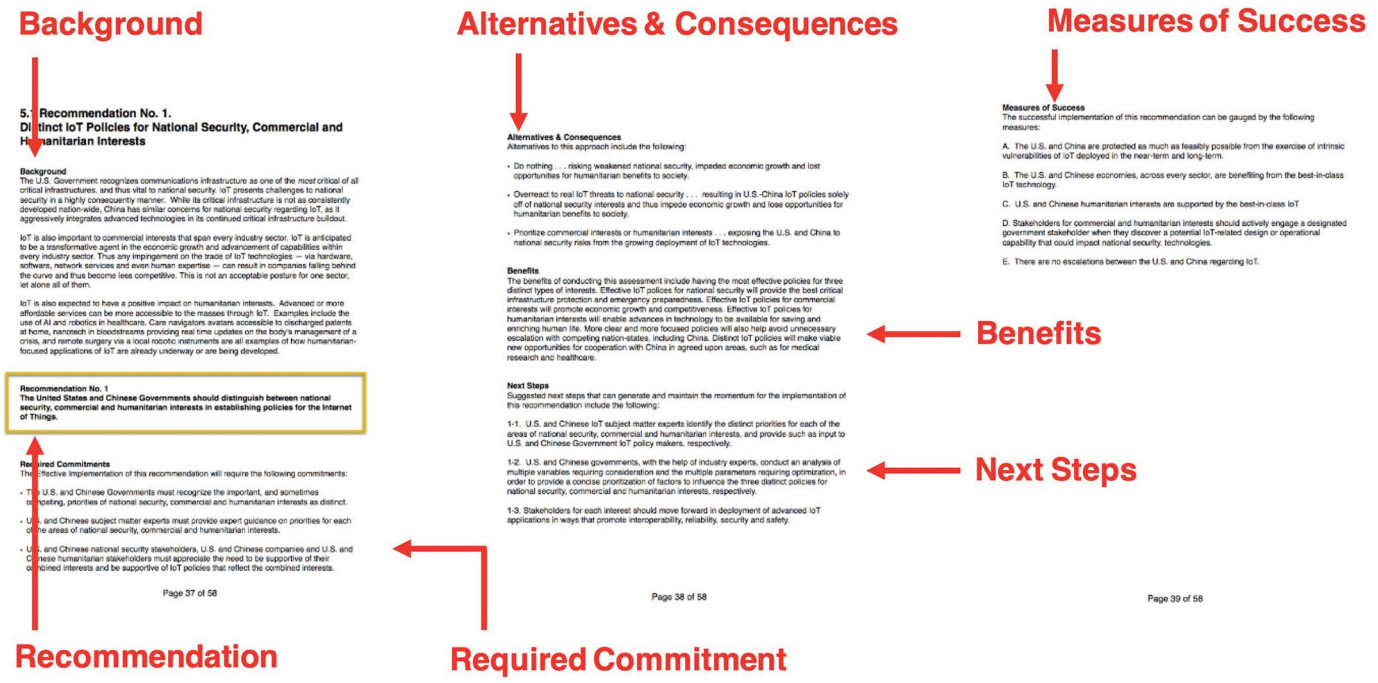


Figure 2. Presentation of Recommendations

A differentiating aspect of the systematic analysis was the use of the Eight-Ingredient (8i) Framework and intrinsic-vulnerabilities approach. Important features of this approach include the following.

A. Proactive in orientation toward threats.

In sharp contrast to conventional approaches used for cyberspace safety and security, which are based on reactions to discovered threats, this proactive approach focuses on intrinsic vulnerabilities. Safety and security are managed by protecting intrinsic vulnerabilities from being exercised, independent of reaction to any specific threats.

B. Comprehensive in a highly complex arena.

In comparison to conventional approaches for managing complex problems, including cyberspace, this approach is comprehensive. The number of intrinsic vulnerabilities in cyberspace, and thus for IoT, is finite. Because any threat must exercise an intrinsic vulnerability to have an effect, a focus on intrinsic vulnerabilities enables complete coverage, independent of threat knowledge.

C. Proven effective.

The 8i Framework and intrinsic-vulnerability approach have proven effective across multiple high-profile and high-consequence applications. Examples include

- the US President's National Security Telecommunications Advisory Committee Report on Next Generation Networks (NSTAC, 2006);
- the Availability and Robustness of Electronic Communications Infrastructures (ARECI) Report, (European Commission, 2007);
- the Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report (IEEE, 2010);
- China-US Bilateral on Cybersecurity: Fighting Spam to Build Trust (EastWest Institute & Internet Society of China, 2011);
- Russia-US Bilateral on Critical Infrastructure Protection—Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace (EastWest Institute and the Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia, 2011);
- Priority International Communications (PIC)—Staying Connected in Times of Crisis (EastWest Institute, 2012);
- China-US Bilateral on Cybersecurity: Frank Communications and Sensible Cooperation to

Stem Harmful Hacking (EastWest Institute & Internet Society of China, 2013); and

- Russia-US Bilateral on Cybersecurity—Critical Terminology Foundations, I & II (EastWest Institute & Information Security Institute of Moscow State University, 2011, 2014).

Problem Solving

The third stage was problem solving, where the solution space was explored for the most positive, impacting, and feasible paths. Here, recommendations were forged based on the preceding meticulous analysis, through an understanding of what is possible with the technology, what is desirable for business, and what is within the grasp of diplomacy in the current situation.

Section 4 presents four recommendations. Each recommendation is introduced with a background that concisely describes the problem being addressed, the required commitments by stakeholders, alternatives and consequences, benefits of implementing the recommendation, next steps to generate momentum, and measures of success for accountability.

Report Generation and Outreach

The final stage of the methodology was the creation of this report and outreach. The report was prepared for an audience of senior policymakers in the United States, China, and other nation states, as well as other stakeholders in government and industry, and the general public—the ultimate stakeholders. Outreach to critical stakeholders regarding the report's recommendations is planned for the first half of 2020, in both China and the United States.

Apparently there is nothing that cannot happen today.

MARK TWAIN

3. Key Observations

This section presents eighty-three objective observations about IoT. More observations could be presented; however, those below are critical for understanding the current situation and anticipating how this technology could affect public safety and national security. The observations span the dimensions of technology, consumers, business, government, and politics. Both the potential benefits of best-case scenarios for IoT and the potential pitfalls of the worst-case scenarios are determined by these factors and how they are managed.

Each observation is utilized as input in the systematic analysis described in Appendix A, and cited in the recommendations presented in Section 4.

3.1 OBSERVATIONS REGARDING TECHNOLOGY

The first set of observations concerns technology. IoT is, first and foremost, based on revolutionary technology; thus, it makes sense to establish a foundation of knowledge about the parameters and trends of the technology.

Key Observation 1. Best-Case Scenario for IoT Technology

The best-case scenario for IoT technology is that every important "thing" is connected and able to provide its intended functionality, and that this connectivity is reliable under normal conditions, robust during extreme stresses, resilient after extreme stresses, and secure against the exercise of intrinsic vulnerabilities within feasible limits.

Key Observation 2. Worst-Case Scenario for IoT Technology

The worst-case scenario for IoT technology is that not every important "thing" can be connected or provide its intended functionality, and that this connectivity is not reliable under normal conditions, not robust under extreme stresses, not resilient after extreme stresses, and not secure against the exercise of intrinsic vulnerabilities within feasible limits.

Key Observation 3. "Things" Means Things

Any thing that is, or can be, deemed important is a candidate for being networked (i.e., becoming part of the IoT), including

- planes, trains, and automobiles;
- forests, farms, and factories;
- people, pets, and plants;
- oceans, atmosphere, and space;
- wearables, hear-ables and eat-ables;
- refrigerators, retail, and retirement communities;
- chat bots, robots, parking spots, and hospital cots;
- smart appliances, smart medicine, and smart cities; and
- shipping containers, packages, and nanotechnology in blood.

Key Observation 4. Oodles of Connected Nodes

IoT is introducing an ever-growing number of nodes (e.g., sensors, devices, and smart machines) that will communicate with one another. These nodes are connected to the Internet, meaning they can potentially be accessed by any other node on the Internet.

Key Observation 5. IoT Plans are Colossal

The Internet-addressing scheme needs to expand so that people do not need to be concerned about running

The number of unique addresses is on the order of

100,000,000,000,000,000,000,000,000,000,000,000

out of unique addresses for the various things hooked up to the Internet. The current Internet-addressing scheme, Internet Protocol Version 4 (IPv4) provides for approximately one billion unique addresses, an amount comparable to the world population. Anyone with a smartphone, laptop, and smartwatch is using three unique addresses. In Internet Protocol Version 6 (IPv6), visionaries of the Internet's future provide one "undecillion" unique addresses. To understand the magnitude of this number, imagine that the population of the world increased by a factor of one thousand (trillions instead of billions), then each person could have one trillion times a trillion unique addresses!

Note that having more addresses does not address the bandwidth needed to move data nor the processing power to run applications.

Key Observation 6. Low-End IoT Technology Provides Data

Some IoT nodes are relatively simple, low cost, and even disposable. Examples of simple devices include sensors that transmit information one way. These can be sensors used for security that indicate whether a window or door is open or closed, or sensors used in agricultural fields that indicate whether moisture is below a certain threshold.

Key Observation 7. Mid-Level IoT Technology Provides Functionality

Mid-level IoT technology includes some data-processing capability.[1] These IoT nodes are, thus, more sophisticated than low-end nodes. Such devices may transmit information two ways (i.e., receive and send) or have some decision-making functionality. A trend is under way for architectures to include more computing at the network's edge, such as via IoT devices.[2]

Key Observation 8. High-End IoT Technology Provides Control

High-end IoT technology competes with, and can even go beyond, human functionality. These IoT nodes are highly sophisticated, utilizing high amounts of bandwidth and performing highly valued functions. Examples of high-end IoT devices include self-driving vehicles that communicate with each other, humanoid service robots that learn to perform an ever-growing number of skills, and avatars that serve as human-like advisors that perform such functions as navigating medical care for patients in their homes.

Key Observation 9. Everything Connected to Everything

Everything that is connected can potentially be accessed and controlled by any other entity that is connected. Various countermeasures can be implemented to prevent such access and control, but the potential is always there.

Key Observation 10. Open-Air Network Interfaces

Many IoT devices will use mobile networks, WiFi, low-power wide-area (LPWA), or other wireless connections to the Internet. This wireless connectivity applies to both low-end devices, such as sensors, and high-end devices, such as robots.

Key Observation 11. Future Mobile Networks are Primarily for Machines

The fastest functions of the human brain are performed by its vision system. As current 4G networks can provide high-definition (HD) video, the threshold for maximum human appreciation for data rates has been met. Thus, the data speeds of future networks are largely for machines that can "think" faster than humans and also handle much larger amounts of data. Future communications networks will be built primarily for handling the traffic of machine-to-machine communications.[3] This is important for understanding what will drive the economics of future infrastructure build-outs.

1 Currently, most mid-level IoT devices use standard processor chips with reduced-instruction-set computing (RISC) architectures. In the coming years, more specialized chips are anticipated to support the vastly expanding special needs of IoT devices. These chips are expected to be designed for low power consumption and low cost.

2 In addition to network architectures supporting edge computing, architectures may become less structured, allowing for mesh networks. Furthermore, these mesh networks may be dynamic, being formed and dismantled on an assented basis. Thus, IoT will make possible more responsive, flexible, and intelligent solutions—though at the cost of increased complexity.

3 Bill Huang, "Robots with Their Heads in the Cloud," *Scientific American*, August 2, 2017, https://tinyurl.com/y6v2bmsr.

Key Observation 12. 5G Mobile Networks Enable High-End IoT

5G networks will greatly increase the capacity of "last mile" access for both the ingress and egress of high-bandwidth traffic. 5G data-transfer rates may be as high as 100 gigabits per second (Gbps)—one thousand times faster than 4G mobile networks. The implication for IoT is that high-end applications will be possible in the near future.[4]

Key Observation 13. Non-Deterministic Bandwidth Utilization

Unlike the world's first telephone-communications networks, for which engineers used deterministic math to size the capacity of networks and predict and control performance, today's networks are increasingly nondeterministic, meaning that it is very difficult to model and plan for how much bandwidth connected devices will use.[5]

Key Observation 14. Non-Deterministic Time of Utilization

In addition to the amount of bandwidth utilized, the timing of the usage is also highly unpredictable. In the old telephone system, it was known that Mother's Day was the day with the heaviest traffic. Furthermore, predictable spikes in traffic were known to occur during weekdays, corresponding to calls made in the early morning and before and after lunch. Some behaviors, like many people setting their IoT speaker's alarm clock to 6 a.m., can be predicted and the spike in network activity anticipated; however, many other behaviors cannot be predicted. Thus, when high bandwidth utilization occurs is nondeterministic.

Key Observation 15. High Bandwidth Consumption

High-end IoT applications (e.g., humanoid robots) may use on the order of 100 megabits per second (Mbps) for applications such as multi-angle real-time computer vision. This is far more than today's HD video applications, which are in the range of 10 Mbps.

Key Observation 16. Machines Fending for Themselves

IoT devices do not typically coordinate their use of bandwidth with other machines. Thus, high-end devices that have the capacity for high bandwidth consumption can have colliding demands for limited throughput capacity. There are currently few or no "gating" functions to smoothly limit the aggregate attempts to prevent congestion. Congestion causes some requests to fail in whole or in part, followed by reattempts. This adds even more congestion and, thus, compounds the problem.

Key Observation 17. Perfect Storm for Congestion

The number of IoT nodes, the high bandwidth consumption of high-end applications, the nondeterministic nature of IoT-device data usage, and the uncoordinated use of bandwidth among these nodes are all factors that converge to increase the frequency with which the intrinsic vulnerability of networks capacity limits will be exploited by natural or manmade threats, resulting in congestion. This congestion will result in traffic delays at best, and outages at worst.

Key Observation 18. Distributed Denial-of-Service Attacks

The susceptibility of IoT devices to be used in DDoS attacks has already been observed.[6] In these incidents, malicious actors exercise the intrinsic vulnerabilities of mutable code in software, the misauthentication and extreme loads of payload, and (most of all) the interconnection and capacity limits of networks.

Key Observation 19. Blockchain for Security

Technology companies have introduced advanced concepts of using blockchain-ledger systems to provide enhanced security for the identity of IoT devices, and for the data created, stored, and in motion between IoT devices. The blockchain-technology approach makes use of a cryptographically secured,

4 5G increases the bandwidth on the first leg of wireless, but does not address bandwidth beyond that point, nor does 5G address the needed processing power for the applications. 5G is not the end-all, and a sixth generation of mobile network standards is expected in a few years.

5 For many decades, the "plain old telephone service" (POTS) line always used a predictable 52 kilobits per second (Kbps) of bandwidth. When the iPhone was initially introduced into AT&T's mobile network in 2007, 4 percent of the users were consuming more than half of the bandwidth. Fred Vogelstein, "Bad Connection: Inside the iPhone Network Meltdown," *Wired*, July 19, 2018, www.wired.com/2010/07/ff-att-fail/.

6 An often-cited example is the Mirai malware and its variants. This malware can turn devices running on the Linux operating system into bots and, in aggregate, form a botnet. Mirai appeared in 2016 and exploited home IoT devices resulting in wide-scale network impairment.

immutable distributed ledger and consensus. It also offers automated optimization of resources.[7]

Key Observation 20. No Babysitters for Devices

In contrast to the components of communications infrastructure today, many IoT devices will not be under observation, nor close protection. Today, network equipment is in locked buildings, and people keep constant guard over their computers and personal smartphones. However, communications infrastructure is about to be inundated with connections to a vast and ever-growing number of IoT assets that are out in the open, with essentially no protection from being accessed.

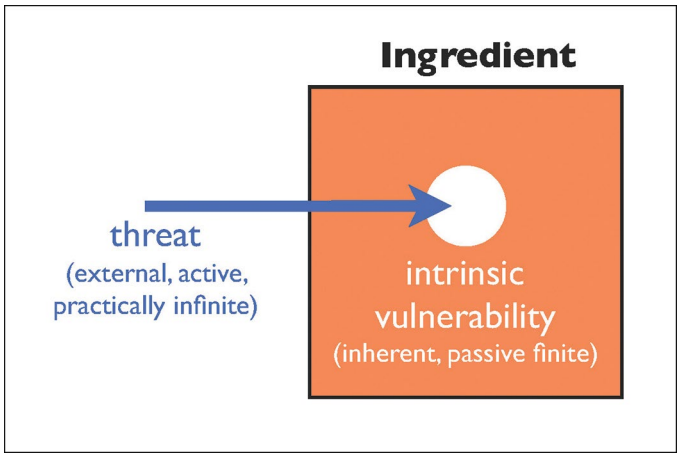
Key Observation 21. Too Many Cooks in the Kitchen

IoT nodes will often run identical or equivalent algorithms. One of the difficult-to-anticipate consequences of such algorithm deployment is that multiple nodes may respond simultaneously when conditions exist at which the algorithms take simultaneous actions. Once a trigger event occurs, and the algorithms all jump in at the same time, the combined response would drive the behavior to overshoot the optimal response.

There are historic precedents for this phenomenon. One notable instance was a major outage in the United States in 1991, in which the automated recovery responses to an overload message created a snowball effect.[8] Another example is the not-infrequent blaming of stock-market volatility on automated trading programs, which can result in loses billions of dollars within a few minutes.

Key Observation 22. IoT is an Extension of Cyberspace

The IoT is an extension of cyberspace.[9] Like other forms of cyberspace, IoT is made up of eight ingredients; a ninth is not essential, and it will not work with any combination of only.[10]



Key Observation 23. The IoT has a Finite Set of Intrinsic Vulnerabilities

Each of the eight ingredients of cyberspace, and by extension IoT, has distinct scientific properties for which there are a finite number of intrinsic vulnerabilities.[11] In contrast to the practically infinite number of threats, the finite number of intrinsic vulnerabilities provides an orthogonal approach to dealing with the complexity of cyberspace.[12]

Examples of intrinsic vulnerabilities for each of the eight ingredients include

- accessibility associated with the environment ingredient;
- grounding and loss of connectivity in the power ingredient;
- design errors residing in the hardware ingredient;
- mutability of code in the software ingredient;
- capacity limits residing in the network ingredient;

7 Applying blockchain to IoT involves having records via a distributed system for sharing data among stakeholders, integrating business terms and conditions for automating interactions between system nodes, implementing hashes for verification of identity and provenance authentication, and establishing consensus agreements for policies for handling bad actors and other threats.

8 The outages were caused by common-channel signaling (CCS) systems in the AT&T network. The response was increased regulatory oversight of the industry. In January 1992, the US Federal Communications Commission (FCC) convened the Network Reliability Council, whose successor Federal Advisory Committee Act (FACA) council (now the Communications Security, Reliability, and Interoperability Council) still survives.

9 "Things" themselves are not necessarily included. For example, a pet cockapoo embedded with a mobile chip is a thing connected to IoT, but not the IoT itself.

10 See Figure 1, Eight-Ingredient (8i) Framework, Section 2.3, *Methodology of the Report;* Rauscher, "Proceedings of the 2001 IEEE Technical Committee on Communications Quality & Reliability (CQR) International Workshop."

11 Rauscher, "Protecting Communications Infrastructure."

12 The number of intrinsic vulnerabilities across all eight ingredients is on the order of one hundred.

- mis-authentication in the payload ingredient;
- divided loyalties in the human ingredient; and
- mis-implementation in the policy ingredient.

Key Observation 24. Threats to IoT Constrained to Intrinsic-Vulnerability Exploitation

Threats are the active agents that exercise passive intrinsic vulnerabilities. With permutations of parameters and their ever-evolving nature, the threats are practically infinite, whereas the intrinsic vulnerabilities are finite.[13] However, despite their vast and ever-growing number, all of the possible threats to IoT—from the past, present, or future—can only cause a reliability or security problem by means of exploiting an intrinsic vulnerability. This constraint provides great insight for understanding the limits and most effective means of dealing with threats to IoT.

The many threats can be categorized as having natural (N) or manmade (M) causes. The latter category can be further subcategorized as either intentional (Mi) or unintentional (Mu). Decades of experience have revealed that the overwhelming majority of problems in cyberspace have had natural and unintentional causes. Intentional manmade threats caused a small minority of problems, even though they receive disproportionate attention.

Examples of threats include

- a flood (N), which exploits the intrinsic vulnerabilities of the power ingredient;
- a backhoe fiber-optic cable cut (Mu), which exploits the accessibility and destructibility intrinsic vulnerabilities of the environment and hardware ingredients, respectively;
- software-design error (Mu), which exercises the logical-design intrinsic vulnerability of the software ingredient; and
- DoS attack (Mi), which exploits the capacity limits of the network ingredient.

Key Observation 25. Cybersecurity is Misplayed as a Reactive Sport

Nearly all cybersecurity is practiced with methodologies based on reacting to threats—effective threat detection and reaction times. This is in sharp contrast to the methods based on the underlying science of the ingredients of cyberspace and the inherent vulnerabilities therein. To use the highly consequential September 11, 2001, terrorist attack as an example, the latter approach would identify the cockpit door as a vulnerability requiring attention prior to any incident, whereas the former approach reacts to threats after they have been exercised, which is too late.

Key Observation 26. International Synergy around Technology is Well Under Way

It is obvious to most scientists and engineers that cooperation with peers often leads to new insights and discoveries. Synergy is achieved through exposure to new perspectives, rigor in thinking, and assistance in developing solutions. Cooperation among peers in IoT and the related fields of next-generation mobile networks, AI, and robotics has been well under way for many years. Ideas are exchanged at thousands of international workshops and conferences held annually, with participants from the United States and China, as well as many other countries.[14] People participate because these events are valuable, and value is exchanged. Along with physical conferences, there are also countless virtual venues where collaboration, and often synergy, is achieved.

3.2 OBSERVATIONS REGARDING CONSUMERS

IoT addresses the migration of the Internet from primarily serving humans directly to primarily serving a multitude of inorganic autonomous devices. This migration has, and will continue to have, a nontrivial impact on consumers. The following observations concern the interests of consumers, the largest stakeholder group for IoT. IoT is being built for them, and consumer adoption of IoT is essential. Trust is a theme across many of these observations.

13 Rauscher, "Protecting Communications Infrastructure."

14 Just one organization, the Institute for Electrical and Electronic Engineers (IEEE) "sponsors more than 1,800 annual conferences and events worldwide." Taken from "Conferences," IEEE, January 30, 2019, www.ieee.org/conferences/index.html#ieee-meetings,-conferences-&-events-(mce)-overview. The author acknowledges that not all of these events address IoT or related technologies, but suggests many do and, thus, thousands is the best order-of-magnitude estimate.

Key Observation 27. Best-Case Scenario for IoT Consumers

The best-case scenario for consumers regarding IoT is that the technology design, operations, commercial practices, and government policies effectively protect their privacy, security, and safety, while providing affordable, high-quality IoT products and services that connect any "thing" important to them. Advanced healthcare and other services not otherwise affordable are now accessible to the masses.

Key Observation 28. Worst-Case Scenario for IoT Consumers

The worst-case scenario for consumers regarding IoT is that the technology design, operations, commercial practices, and government policies fail to effectively protect their privacy, security, and safety, and result in overly expensive, poor-quality IoT products and services that do not connect any "thing" important to them. Advanced healthcare and other services remain beyond the reach of the masses.

Key Observation 29. Consumer Adoption of IoT is Vital

Consumers are the largest stakeholder group for IoT. In the United States alone, the number of smart-home devices is estimated to surpass one billion by 2023, with consumers dishing out nearly $1 trillion for IoT solutions.[15] This adoption is key to the anticipated roll-out of IoT proceeding as predicted.

Key Observation 30. Consumers are a Mixed Bag

When it comes to important factors that could affect a given consumer's relationship with IoT, several factors will weigh heavily on adoption and use. These factors include financial resources, home environment, prioritization of convenience vs. security, and familiarity and comfort with technology. It is important to note that, for each of these factors, there is a wide spectrum of consumers; they are not monolithic in the marketplace.

Key Observation 31. Early Adopters Opt for Convenience

The rapid adoption of social media and other Internet-based services demonstrates the prioritization that many consumers place on expedience. For many consumers, the trade-off of security for convenience was not a long deliberation, if it was one at all. For slower adopters, participation in some social media was eventually necessary, but it required a leap of faith. Still others remain holdouts. Economists have long observed the irrational decision-making behavior of consumers in the marketplace.[16]

Key Observation 32. IoT Devices Will Operate within Circles of Privacy

IoT devices that can listen to and watch people in their homes and offices are already being adopted on a large scale.[17] IoT devices are expected to continue to be deployed, to an even greater extent, wherever people are doing any activity.

Key Observation 33. People Don't Trust AI

As the general public becomes more familiar with AI, often through IoT chat bots, there is growing consumer concern among a segment of the population about what AI may be doing. Most of the concerns regard privacy, security, and decisions being made without the public's knowledge and approval.

Key Observation 34. People Don't Trust Robots

As the general public becomes more aware of robots having control of their physical environment (e.g., autonomous vehicles), there is a growing sense among a segment of the population that robots may put them in danger.

Key Observation 35. People Don't Trust Big Tech Companies

In the United States, consumer polls indicate that there is a trend of increased distrust of big technology ("Big

15 Shelagh Dolan, "How the Internet of Things Will Transform Consumerism, Enterprises, and Governments Over the Next Five Years," *Business Insider*, July 19, 2018, https://www.businessinsider.com/iot-forecast-book-2018-7. Consumers make 63 percent of purchases, and the estimated 2022 market is $1.2 trillion. Louis Columbus, "2018 Roundup of Inter of Things Forecasts and Market Reports," *Forbes*, December 13, 2018, https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#71bef1567d83.

16 Jon Cummings, Ravi Dhar, and Ned Welch, "Irrational Consumption: How Consumers Really Make Decisions," McKinsey & Company, February 2015, https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/irrational-consumption-how-consumers-really-make-decisions.

17 Examples include Amazon Echo, Apple HomePod, Google Home, Microsoft Cortana, Samsung Bixby, and SoundHound, among others.

Tech") companies. One aspect of the distrust regards how Big Tech businesses are not transparent about how they exploit consumers' personal information and whether the companies are following the law regarding its protection.[18]

Key Observation 36. People Don't Trust Government

In the United States, consumers have a distrust of government.[19] This distrust can be healthy, and is not necessarily considered a problem as the US Constitution is deliberately structured with an assumption that government cannot be trusted, and institutes checks and balances across its divisions of power.

In China, the communist political system requires a distinctly higher level of trust in the government than does the US political system.

Despite fundamental differences in the expectations for trust in government, government leaders in both the United States and China want their respective general publics to trust what they are doing as new technology is introduced. To this end, both governments have a common interest in seeing effective protections in place regarding consumer interests (e.g., safety and security).

Key Observation 37. Unprecedented Trust

Further adoption of emerging technology (i.e., IoT) will require more trust on the part of consumers: trust in technology, including machines and software; trust in companies; and trust in governments. Consumers will be entrusting them with their privacy, physical well-being, and fortune. Whatever trust has been exhibited by consumers thus far, living with IoT will require unprecedented trust.

Key Observation 38. Avatar Knows Best

In a future with more frequent contact with ever-smarter machines, some people may begin to feel detached from other humans, and may seek social interactions with synthetic people (avatars). This could fundamentally change usage and behavior.[20] In addition to an emotional connection, some humans may intellectually trust their peers less and, being so impressed with their intelligence, trust virtual advisors more. Examples of how this could have nontrivial impacts include if the avatar suggests what to buy or how to vote, objectives already attempted via the Internet today.[21]

Key Observation 39. Assassination by IoT

As medical devices are connected to humans and the Internet, there is growing potential for individual or collective assassinations. Pacemakers and insulin pumps are obvious devices that can be steered to kill their users.[22]

3.3 OBSERVATIONS REGARDING BUSINESS

The following observations concern business—the economics around IoT and the interest of enterprise stakeholders. While fewer in number, enterprise stakeholders have much larger individual spending budgets for IoT products and services than will consumers.

Key Observation 40. Best-Case Scenario for IoT Business

The best-case scenario for IoT business is that there is a long, steady growth of interoperable products and service offerings, introduced with ever-shorter cycle times, in a fair marketplace in which competition thrives. The economy prospers across many sectors.

Key Observation 41. Worst-Case Scenario for IoT Business

The worst-case scenario for IoT business is that there are choppy ups and downs in product and service offerings, which do not interoperate, and unfair market practices stifle competition. Economic development is unfortunately stunted.

18 Asunción Esteve, "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA," *International Data Privacy Law 7*, 1 (2017), 36–47, https://academic.oup.com/idpl/article-abstract/7/1/36/3097625.

19 Only 18 percent of Americans today say they can trust the government in Washington to do what is right "just about always" (3 percent) or "most of the time" (15 percent). See "Public Trust in Government: 1958-2017," Pew Research Center, December 14, 2017.

20 Kate Darling, "Extending Legal Rights to Robots, Will Projecting Emotions onto Objects Lead to an Extension of Limited Legal Rights to Robotic Companions?" *IEEE Spectrum*, 2012.

21 For insights in to how user profiles are used to present search responses see Marsali Hancock, "Why Student Data Privacy Matters," *GIIC Insights*, May 25, 2017, giic.org/why-student-data-privacy-matters/.

22 Ms. Smith, "Hacking Pacemakers, Insulin Pumps and Patients' Vital Signs in Real Time," CSO, August 12, 2018, www.csoonline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html.

Key Observation 42. Money Magnet

Overall investment in IoT is expected to be on the order of $10 trillion by 2025.[23]

Key Observation 43. Connected Intelligence

Similar to how previous industrial revolutions provided key values such as increased productivity of goods via machinery and access to vast information, the IoT revolution now under way is fundamentally about connecting intelligence.[24]

Key Observation 44. A Unicorn Stampede

While the emerging technology areas of 5G, AI, and robotics are anticipated to bring about exponential economic growth, their intersection will be even more disruptive and economically potent. It is not yet known what the new services will be. However, careful analysis of existing markets, potential for growth, and past and present trends indicate that the IoT is likely to spawn hundreds of new $1-billion-plus companies.[25]

Key Observation 45. Cloud Robotics is the Killer App for IoT

Cloud robotics is the concept of many robots sharing a common brain (comprising many AI engines) in the cloud.[26] Here, the cloud brain and robot form a symbiotic relationship—the former learning new skills from its many robots, and the latter downloading the new skills learned from other robots. The bandwidth of 5G and the feasibility to connect many robots to many AI engines in the cloud make cloud robotics viable. Because of the high value of a humanoid robot that can continuously learn new skills and perform endless tasks that people prefer not to do—and also tasks that are beyond what humans can now do—such an IoT application will likely be the "killer app" for IoT.[27]

Key Observation 46. High-End IoT will Drive Massive New Infrastructure Deployment

As the high-bandwidth capacity of 5G brings explosive growth in the amount of data created and transmitted from and to networks' edges, the demand for capacity in core networks will mushroom. The accelerated growth in demand for handling core network traffic requires enormous increases in core-infrastructure capacity and, thus, significant investment in core infrastructure.

Key Observation 47. Limited Core Network Capacity Can Impede IoT Progress

Limitations in core-infrastructure capacity could impede the advancement of IoT by either lacking sufficient capacity, having sufficient capacity but at too high a cost, or having inconsistent access to required capacity. Any of these cases could make high-end IoT applications unreliable.

Key Observation 48. Data is the New Oil, the New Gold, and the New Black

The increased collection of mountainous stores of data promises to unlock untold fortunes. At a fundamental level, IoT is actually valuable because data is valuable. In turn, data is valuable because it can enable intelligence—both human and artificial. Like oil, data will be a new commodity. Like gold, it will be traded in commerce. And, like black, it will sometimes be like fashion, limited to the value of its perception.[28]

Key Observation 49. More, Better Sensors on the Cheap

As the demand for large volumes of sensors takes off, the price per device will drop. The expanding market for IoT solutions will drive innovation to create new and better sensors. Thus, areas for the sensor business are

23 Peter Newman, "The Internet of Things Report: Technology Trends & Market Growth," *Business Insider*, July 27, 2018, https://www.businessinsider.com/internet-of-things-report.

24 This understanding is a refinement from the early days of the IoT vision, when the focus was on passive sensors sending data to a remote location for processing. The drop in computing-resource costs and the new high bandwidth of 5G have increased the viability of edge computing for many applications. Edge computing will also reduce the cost of network-transport and cloud-storage resources. Depending on whether 5G networks deliver on their bandwidth promises, the lower latency of edge computing devices could be an attractive feature.

25 "Proceedings of the Mobile Future Forward Summit," Chetan Sharma Consulting, 2018.

26 The term "cloud robotics" was coined in 2010 by James J. Kuffner, Jr., adjunct associate professor at the Robotics Institute at Carnegie Melon University and CEO of Toyota Research Institute—Advanced Development (TRI-AD), to describe how network-connected robots could learn and access shared skills via distributed computation and data stored in the cloud.

27 The term "killer app" refers to the use case that justifies a larger technology platform.

28 A 2018 Gartner study found that 35 percent of IoT projects were selling or anticipating selling data collected. "Gartner Identifies Top 10 Strategic IoT Technologies and Trends," Gartner, press release, November 7, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

the conventional areas of research, development, and manufacturing.

Key Observation 50. Devices are Participants in Open Markets

Some sensors or smart devices may need the data or intelligence from other, similar entities. It is envisioned that such devices will have access to open markets where, for a micro-fee, they can purchase what they need to perform their function.

Key Observation No. 51. Digital Twins

A likely field for many new businesses is the design and operation of realistic virtual representations of systems, such as airplanes, factories, or household humanoid robots. The "digital twin" will be supported with historic and real-time data fed into machine-learning algorithms that generate insights and predictive models. The result allows operators to have advance warning of the potential for component failure, automatically schedule and perform maintenance, and, thus, reduce downtime and improve efficiencies. The concept may also apply to a human body.

Digital twins pose a new threat for malicious activity against critical-infrastructure systems. If an adversary were able to glean sufficient data for a system, it could use the digital-twin predictive model for nefarious purposes.

Key Observation 52. Early Adopters are Retail, Healthcare and Supply-Chain Sectors

The initial industrial sectors that are poised to see the fastest growth in IoT applications are retail, healthcare, and supply chain.[29] In these industries, IoT can quickly become the backbone for delivering value to customers, making the value proposition straightforward. IoT can immediately enhance value for these sectors in very direct ways.

Key Observation 53. Software from Everywhere

The development of "skills" for smart machines will be accomplished via software—specifically, AI. The software for such skills can be developed in any place software programmers live. In most cases, this software will be maintained via software updates from developers across a range of locations. Thus, the AI utilized by IoT will likely be sourced from locations in many nation states.

Key Observation 54. China a Leader in Manufacturing

China is the largest manufacturer of communications-network equipment in the world.[30] China's Huawei is the world's leading supplier of telecom equipment. Given its industrial base, experience, and competitive cost structure, China is expected to be the leading manufacturer of IoT devices for the foreseeable future.[31]

Key Observation 55. United States Leads in Innovation

The United States continues to lead the world in innovating extensions of the Internet.[32] This leadership position is expected to continue in the near future. However, China and other countries that are strategically investing in technology innovation are expected to develop increasingly impressive capabilities to accomplish breakthroughs in technology.[33]

Key Observation 56. Opportunity to Lead in Early Adoption

For some sectors, such as healthcare, there exist significant regulatory hurdles for businesses seeking market entry with a new product. Regulations are often out of date, and do not anticipate the benefits associated with early adoption of new technologies, such as insights gleaned, early understanding of trends, faster

29 Columbus, "2018 Roundup of Inter of Things Forecasts and Market Reports"; Allison DeNisco-Rayome, "The Five Industries Leading the IoT Revolution," *ZDNet*, February 1, 2017, https://www.zdnet.com/article/the-five-industries-leading-the-iot-revolution/. "94% of Businesses will use IoT by the End of 2021: Microsoft Report," IoT Magazine, August 10, 2019, https://theiotmagazine.com/94-of-businesses-will-use-iot-by-the-end-of-2021-microsoft-report-cf94ad11f173.

30 Arne Holst, "Telecommunication Equipment Companies Ranked by Overall Revenue in 2018 (in Billion U.S. Dollars)," Statista, August 21, 2019, https://www.statista.com/statistics/314657/top-10-telecom-equipment-companies-revenue/.

31 "...Greater China makes most of the sensors, microchips, and other components that are the fabric of the IoT. By 2020, there will be 200 billion IoT connected components and devices globally, of which 95 percent will be manufactured in China..." "How Greater China is Set to Lead the Global Industrial IoT Market," GSM, July 2018, 5, https://www.gsma.com/iot/wp-content/uploads/2018/06/GSMA_Report-How_Greater_China_Is_Set_To_Lead_Global_Industrial_IoT_Market-en-July2018.pdf.

32 "Science & Engineering Indicators 2018," US National Science Board, 2018.

33 Walter Isaacson, "How America Risks Losing Its Innovation Edge," *Time*, January 3, 2019, https://time.com/longform/america-innovation/.

development lifecycles, and influence over standards and other broader policies that will affect the emerging IoT landscape. China, the United States, and other nation states have the opportunity to be leaders in the early adoption of IoT for single or multiple sectors, by significantly reducing regulatory obstacles for entrepreneurs.

Key Observation 57. Supply Chain is Complex and International

While the United States and China are the world's two major cyber powers, the landscape is more complicated than that. Many other countries will contribute to the IoT ecosystem. Both the design and operation of IoT systems will entail many components and processes, with many companies and countries involved.

Key Observation 58. The IoT Lifecycle is a Leaking Sieve of Information

The entire research-and-development (R&D) technology-product lifecycle provides opportunities for technology transfer between countries: teaching the foundations of mathematics and computer programming to research conducted in graduate schools that is published and shared with colleagues; products and services are marketed with descriptions of distinguishing features; patents are achieved via public disclosure in the patent-filing process; and technologists move from one company to another. Thus, it is not possible to stop the innovation of other nation states.

Key Observation 59. Lack of Interoperability is a Major Barrier to IoT Development

IoT products and services are greatly hampered by the lack of interoperability. The lack of agreements, standards, policies, and regulations (ASPR), or "policy" for short, is presently holding back progress more than any hardware or software issues. In order to use more IoT devices, consumers are faced with the need to manage an increasing number of apps and network bridges. Operation and management are further complicated by different security capabilities across devices.

If interoperability is limited to nation-state or company-proprietary standards, the market fragmentation cost of participation for companies is increased, and costs are passed on to consumer and enterprise stakeholders. Refusal to support cooperative ASPR development has been a non-tariff barrier to trade, and is understood, at times, to be intentional.

Key Observation 60. Interoperability Will Be a Watershed Milestone for Businesses

If interoperability can be achieved on a broad international scale, the risk for companies is reduced dramatically, and stakeholders can benefit from lower-cost and more valuable systems. This requires leadership and cooperation that is not currently present. Interoperability enhances connectivity, which is generally a good thing. There is a trade-off, as some would suggest having less connectivity can enhance security, and the cost to these proponents is worth the protection.

Key Observation 61. Data-Aggregation Risks

The past decade has seen a few companies emerge as major aggregators of data.[34] These cloud-service providers are taking on more and more responsibility. With such data aggregation, the potential increases for multiple millions of people being impacted by a single event—service impacts, corrupted data, or other breaches. Such events would have huge impacts on businesses and consumers; the perfect crime could occur if a breach was not detected.

Key Observation 62. Ownership of Cyberspace

While the US government makes pronouncements of its strategy for cyberspace, it is often not immediately apparent in those assertions that, in the United States, private companies own and operate nearly all of the infrastructure that makes up cyberspace. In China, major operators, such as China Mobile, are owned by the state.

Key Observation 63. Revisiting Infrastructure Investment Paradigm

Given the transformative change that IoT brings, some experts suggest the current investment paradigm needs to be revisited, in order to keep pace with technology demands and opportunities.[35] On one hand, governments view driving 5G deployment as key to continued economic growth, and they rely on their licensed carriers to make the deployment happen for the sake of economic progress. On the other hand,

34 The top three cloud-service providers (Amazon, Microsoft Azure, and Google Cloud) hold about 60 percent of total market share. "Canalys Cloud Channels Analysis 2019," Canalys, 2019.

35 Brian H. Thompson, "A Simple Route to Better Internet Infrastructure," *GIIC Insights*, December 6, 2016, http://giic.org/a-simple-route-to-better-internet-infrastructure/.

existing network-operator models may be outdated, and can impede progress.

3.4 OBSERVATIONS REGARDING GOVERNMENT AND POLITICS

This section provides observations about IoT regarding government and politics, with particular focus on the US-China relationship. With such broad subject matter, key observations presented below are those that impact the subject at hand.

Key Observation 64. Best-Case Scenario for IoT Politics

The best-case scenario for IoT regarding the US and Chinese governments is that: each can achieve their respective national security, economic, and humanitarian objectives without sacrificing one interest for the other; both countries avoid a major IoT-related escalation with each other; and the stability and balance of power modeled in the US-China relationship is a positive influence throughout the world.

Key Observation 65. Worst-Case Scenario for IoT Politics

The worst-case scenario for IoT regarding the US and Chinese governments is that: both fail to achieve their respective national security, economic, and humanitarian objectives, and become caught in a cycle of sacrificing one interest for another; both countries have frequent, major IoT-related escalations with each other; and the instability and power struggle of the US-China relationship has a far-reaching, negative influence throughout the world.

Key Observation 66. Both US and Chinese Governments View IoT as Strategic

Like past technological advances, emerging technologies such as IoT, 5G, and AI are considered strategic for economic growth and national security. Technological advances are the pathway to superiority on a number of fronts, and a strong economy is essential for long-term national defense. Both governments want to promote progress and be global leaders in IoT.

Key Observation 67. Made in China 2025

The Chinese government has a strategic plan for comprehensively elevating China's role across a wide range of global industries.[36] The plan includes a focus on high tech.[37] China's plan follows Germany's Industry 4.0 plan to use IoT to improve small and medium-size businesses' capability to be more efficient, agile, and customizable.[38]

Key Observation 68. China Collaborating with International Standards

In recent years, the Chinese government has recognized the strategic advantage of participating in international standards-development processes.[39] On one hand, this adjustment makes Chinese markets more accessible to foreign companies; on the other, it provides Chinese companies with more opportunities to access foreign markets for their products. Importantly, Chinese companies in the IoT space have more flexibility in determining which standards they want to follow.

Key Observation 69. US Innovation is Private-Sector Driven

The US government's role in innovation is minimal. On one hand, it could be argued that government policies in regard to promoting science, technology, engineering, and math (STEM) education have played a critical role. However, on the whole, most innovation is accomplished by private entrepreneurs, and the government helps most when it keeps regulations to a minimum.

Key Observation 70. China Continues to Grow in Influence

China's stature is on the rise in world affairs, bolstered by its sustained economic growth. China is preparing for continued growth in influence in the coming decades, and its political system allows it to do planning for longer terms compared to governments that see more frequent changes in political-party leadership.

36 In May 2015, Chinese Premier Li Keqiang and his cabinet issued a ten-year strategic plan that emphasizes a "Made in China" goal. "Premier Li on 'Made in China 2025,'" State Council, last updated August 10, 2017, http://english.www.gov.cn/premier/news/2017/08/10/content_281475781726536.htm.

37 "'Made in China 2025' Plan Unveiled to Boost Manufacturing," *GB Times*, May 25, 2015, www.gbtimes.com/made-china-2025-plan-unveiled-boost-manufacturing.

38 Scott Kennedy, "Made in China 2025," Center for Strategic and International Studies, June 1, 2015, www.csis.org/analysis/made-china-2025.

39 John Chen, et al., *China's Internet of Things, A Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission* (Reston, VA: SOSi, 2018).

Key Observation 71. Infrastructure Protection a Common Concern

Both the US and Chinese governments consider critical-infrastructure protection an integral part of national security. Further, both governments understand that IoT will play an increasingly important role in critical-infrastructure operations. What both countries have not yet figured out is how to determine what exposure to foreign IoT components is acceptable.

Key Observation 72. AI Is an Integral Part of IoT as a Strategic Economic Advantage

AI is a technology whose value is highly correlated with the rollout of IoT. Many governments have been proactive in stating their intentions to compete economically using AI. Canada was the first to release a national strategy, and many countries have followed.[40]

Key Observation 73. China's National Strategy Concerning AI is Comprehensive

China's strategy for AI may be the most comprehensive of any national plan.[41]

Key Observation 74. Trade Deals Being Renegotiated

US economic policy toward China is undergoing transformation. US President Donald Trump has stated, "From now on, we expect trading relationships to be fair and reciprocal."[42] Aspects of negotiations include market access, sanctions, and respect for intellectual property, all of which have watershed impacts on IoT trade.

Key Observation 75. IoT as Strategic Military Advantage

Many advances in IoT can have military applications. Given that technology has often played a decisive role in past conflicts, any advantage is a serious concern for both the United States and China.

Key Observation 76. International Communications Infrastructure a Target

Electronic-communications infrastructure has been the target of attack since its earliest deployments. Precedent for cutting undersea cables dates back to 1898.[43]

Key Observation 77. Two Schools of Thought

There tend to be two schools of thought regarding the critical infrastructure of an adversary in conflict. On one hand, some argue that damage to critical infrastructure should be avoided during conflict because of the population's reliance on it for human welfare, and those of this persuasion promote a surgical approach to attacks. On the other hand, others argue that such surgical approaches delay the final outcome of a war, and suggest that the disabling of critical infrastructure is more humane because of its ability to accomplish a more decisive outcome more quickly, and avoid prolonging suffering and active conflict.

Key Observation 78. Anyone Can be a Troublemaker

While cyber superpowers like the United States and China have more capabilities to launch a debilitating attack on IoT, other, less powerful, nation states and non-state actors are capable of causing similar harm via asymmetric engagements.

Key Observation 79. Leadership Being Challenged

Recent U.S. policy measures have been advanced to provide defensive measures for "critical emerging" technologies.[44] The release of recent proposed

40 "CIFAR Pan-Canadian Artificial Intelligence Strategy," CIFAR, 2017, www.cifar.ca/ai/pan-canadian-artificial-intelligence-strategy. The following countries have a national strategy for AI: Australia, Austria, Canada, China, Denmark, Estonia, Estonia, Finland, France, Germany, India, Ireland, Italy, Japan, Kenya, Malaysia, Mexico, New Zealand, Russia, Singapore, Saudi Arabia, South Korea, Sweden, Tunisia, United Arab Emirates, United States of America, and the United Kingdom. "National and International AI Strategies," Future of Life Institute, October 2019, https://futureoflife.org/national-international-ai-strategies/?cn-reloaded=1.

41 Guofa, State Council of China. "Notice of the New Generation Artificial Intelligence Development Plan," July 8, 2017, www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

42 "President Donald J. Trump is Confronting China's Unfair Trade Policies," White House, press release, May 29, 2018, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-confronting-chinas-unfair-trade-policies/.

43 Douglas Straight, ed., "Cable Cutting in War Time," *Pall Mall Gazette*, May 11, 1898.

44 S.29 — 116th Congress (2019-2020), *A bill to establish the Office of Critical Technologies and Security, and for other purposes*. www.congress.gov/bill/116th-congress/senate-bill/29/text.

bipartisan legislation was accompanied by an expressed concern: "China and other nations are currently attempting to achieve technological and economic superiority over the United States through the aggressive use of state-directed or -supported technology transfers."[45]

Key Observation 80. Partial IoT Policy Positions

Some advocates for US national security and commercial interests suggest policies that are focused on making sure that China does not surpass the United States in AI and other technologies related to IoT. However, it is difficult, if not impossible, to control what another country does (how much it invests, what it invests in, its strategic imperatives, etc.).

Key Observation 81. US Government Acknowledges Dual-Use Technologies

The US government recognizes that technologies can have both military and civilian applications. The implication is usually that the potential military application makes certain knowledge about technologies sensitive, and possibly requiring controls.

Key Observation 82. Conflation Abounds in AI Chatter

Past complaints against hacking in cyberspace have combined protests against military assets, companies, and hospitals, despite the interests and expectations for these areas being distinct. Policy discussions regarding AI have continued the practice of combining these distinct interests.

Key Observation 83. Historic Analogy Dominates Strategic Policy Development

The September 11, 2001, terrorist attack against the United States was caused, in part, by neglecting to consider threats outside of those historically experienced. Indeed, the cockpit door was a known vulnerability prior to September 11; however, since it had never been used by terrorists before, it was not a priority. The overweighting of historic analogy is an unlearned lesson throughout history.

45 *Rubio, Warner Introduce Bipartisan Legislation to Combat Technology Threats from China*, January 4, 2019. www.warner.senate.gov/public/index.cfm/pressreleases?ID=9D405E99-2E31-4A2D-A79F-9F3FF3B32122.

4. Recommendations

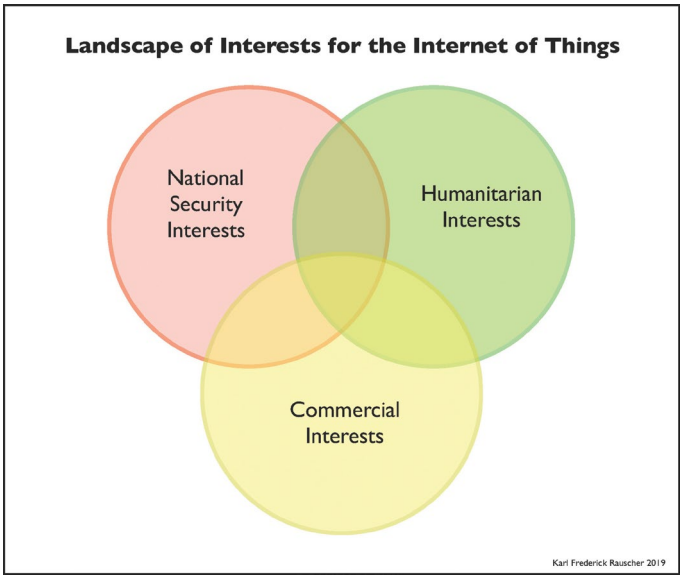


Figure 3. Landscape of Interests in Cyberspace.[46]

This report submits four recommendations. Each recommendation is vital for achieving a world where IoT can fulfill its potential to enhance the lives of humankind with optimum safety, and protect the legitimate national security interests of nation-state governments. Importantly, the recommendations also reflect the conditions necessary for commercial interests to thrive. Each recommendation is actionable and, if implemented, can be effective in dissolving a hitherto unsurmountable obstacle. The report urges stakeholders to give ample consideration, and pursue timely action, for each of these recommendations, as appropriate.

The first recommendation submits that IoT is so common and integral to society that no single interest should dictate policies that seriously impair the ability of stakeholders of other interests to achieve their objectives. In this regard, the first recommendation identifies three primary interests: national security, commercial, and humanitarian (Figure 3, Landscape of Interests in Cyberspace). Each of the remaining three recommendations provides guidance for advancing one of these interests. The second recommendation enhances national security by ensuring that the US and Chinese governments and operators of critical infrastructure can communicate in a crisis, despite IoT greatly increasing the potential for network congestion that could block such critical communications. The third recommendation extends the envelope of US-China cooperation on humanitarian applications of IoT, providing means to cooperate when incidents concern either party. The fourth recommendation paves the way for economic growth by raising the bar for the quality and specificity of any government regulation that could be an obstacle to entrepreneurs.

History and experience tell us that moral progress comes not in comfortable and complacent times, but out of trial and confusion.

US PRESIDENT GERALD R. FORD

4.1 RECOMMENDATION NO. 1.

DISTINCT POLICIES FOR NATIONAL SECURITY, COMMERCIAL, AND HUMANITARIAN INTERESTS IN IOT

Purpose

The purpose of this recommendation is to reveal new opportunities for the pursuit of interests vital to both the United States and China regarding IoT by deconflicting confusion—created by conflation of interests—that has, until now, hindered mutually beneficial realization of both countries' interests.

Background

Like a wheel, IoT can be used for many purposes. Just as a wheel can be used as an integral part of the landing gear of a stealth bomber, the local pizza-delivery fleet, or an ambulance, IoT concepts and technologies are used to network battlefield assets, track supply-chain inventory in real time, and extend advanced healthcare via outpatient medical devices.

The US government recognizes communications infrastructure as one of the most critical of all critical infrastructures, and, thus, vital to national security.

46 The initial version of this diagram appeared in Rauscher and Yonglin, "China-U.S. Bilateral on Cybersecurity."

Accordingly, IoT presents challenges to national security that can have grave consequences. While its critical infrastructure is not as consistently developed nationwide as is that of the United States, China nonetheless holds similar concerns about national security in the face of IoT, as the country aggressively integrates advanced technologies in its continued critical-infrastructure build-out.

The impending IoT upheaval is also highly important to commercial interests across every sector of industry. IoT is anticipated to be a transformative agent in the economic growth and advancement of capabilities within every industry sector. Thus, any contrived impingement on the trade of IoT technologies—via hardware, software, network services, and even human expertise—can result in companies losing their competitive edge. This is an untenable posture for one sector, much less all of them. Both the United States and China are vulnerable to IoT policies that negatively affect their economies in such a pivotal domain.

IoT offers highly valuable benefits for human welfare. Advanced or more affordable services can be more accessible to the masses through IoT. Healthcare is one of the top sectors anticipated to be an early adopter of IoT. Connected AI applications are extending the reach of limited medical-care professionals, and online robotics are enhancing their skills.[47] The citizens of the United States and China would be ill served if government policies significantly impede robust use of IoT for their welfare.

On an international level, the current discussion on IoT safety and security often conflates the distinct interests of national security, business, and human welfare. This blending of distinct needs results in ineffectual and stagnating approaches to problem solving.

The recommendation engages IoT by recognizing the profound potential for each of the three interests. The recommendation is actionable in that all of the required commitments are reasonable and possible. The recommendation is bold, in that it rebukes a common practice and sets the stage for a more rigorous—but also more helpful—framework for managing competing IoT interests.

RECOMMENDATION NO. 1

The United States and Chinese governments should distinguish between national security, commercial, and humanitarian interests in establishing policies for the Internet of Things.

Required Commitments

The effective implementation of this recommendation will require the following commitments.

- The US and Chinese governments must recognize the important, and sometimes competing, priorities of national security, commercial, and humanitarian interests as distinct.
- US and Chinese subject-matter experts must provide expert guidance on the priorities for each area of national security, commercial, and humanitarian interests.
- US and Chinese national security stakeholders, commercial stakeholders, and humanitarian stakeholders must appreciate the need to support their combined interests, and support IoT policies that reflect them.

Alternatives and Consequences

Alternatives to this approach include the following.

- Do nothing, risking weakened national security, impeded economic growth, and forfeited opportunities for humanitarian benefits to society.
- Overreact to real IoT threats to national security, resulting in US-China IoT policies shaped solely by national security interests and, thus, impede economic growth and lose opportunities for humanitarian benefits to society.
- Prioritize commercial interests or humanitarian interests, exposing the United States and China to national security risks from the growing deployment of IoT technologies.

Benefits

The benefits of conducting this assessment include having the most effective policies for three distinct types of interests. Effective IoT polices for national security will provide the best critical-infrastructure protection and emergency preparedness. Effective

47 Care-navigator avatars accessible to discharged patents at home, nanotech in bloodstreams providing real-time updates on the body's management of a crisis, and remote surgery via local robotic instruments are all examples of how humanitarian-focused applications of IoT are already under way or are being developed.

IoT policies for commercial interests will promote economic growth and competitiveness. Effective IoT policies for humanitarian interests will enable advances in technology to be available for saving and enriching human life. Clearer and more focused policies will also help avoid unnecessary escalation with competing nation states. A segmented approach to IoT policy provides new opportunities for cooperation between the United States and China in agreed-upon areas identified as having low risk, low cost, and high reward, such as for medical research and healthcare.

Next Steps
Suggested next steps to generate and maintain momentum for the implementation of this recommendation include the following.

1-1. US and Chinese IoT subject-matter experts identify the distinct priorities for each of the areas of national security, commercial, and humanitarian interests, and provide such as input to US and Chinese government IoT policymakers.

1-2. The US and Chinese governments, with the help of industry experts, conduct an analysis of variables requiring consideration and the multiple parameters requiring optimization, in order to provide a clear structure for factors to influence the three distinct policies for national security, commercial, and humanitarian interests.

1-3. Stakeholders for each interest should move forward in deployment of advanced IoT applications, in ways that promote interoperability, reliability, security, and safety.

Measures of Success
The successful implementation of this recommendation can be gauged by the following measures.

A. The United States and China have IoT policies that reflect the distinct interests of national security, commerce, and human welfare.

B. The United States and China have policies that enable their respective economies to benefit from the deployment of best-in-class IoT technology.

C. US and Chinese humanitarian interests are supported by best-in-class IoT.

D. US and Chinese stakeholders for commercial and humanitarian interests actively engage a designated stakeholder for their respective governments, when they discover a potential IoT-related design or operational capability that could impact national security.

E. Security concerns between the United States and China regarding IoT stay in the respective lanes of national security interests, commercial interests, or humanitarian interests, and avoid unnecessary escalation.

If everything is important,

then nothing is.

- PATRICK LENCIONI, AUTHOR

4.2 RECOMMENDATION NO. 2

PRIORITY SCHEME FOR CRITICAL HUMAN AND MACHINE COMMUNICATIONS

Purpose
The purpose of this recommendation is to address network congestion, the most glaring aspect of IoT for emergency preparedness in an international crisis.

Background
The nature of national security being what it is, the United States and China have, chiefly, competing interests in this arena. There are some exceptions where interests are aligned, such as stemming nuclear-weapon proliferation, avoiding conflict escalations in the world, and promoting global economic stability. In these areas, focused cooperation has been achieved. The introduction of IoT creates at least one new area where national security interests should be aligned: ensuring critical US-China communication in a crisis.

Communication is fundamental to any level of cooperation. The transformative effect of IoT on communications has, among its many facets, a radical impact on network traffic. This factor provides the conditions for a perfect storm for frequent outages due to congestion that occurs when the statistical variation of data traffic spikes above capacity thresholds.

Not all traffic is the same. Given the anticipated critical function of some connected entities, some traffic

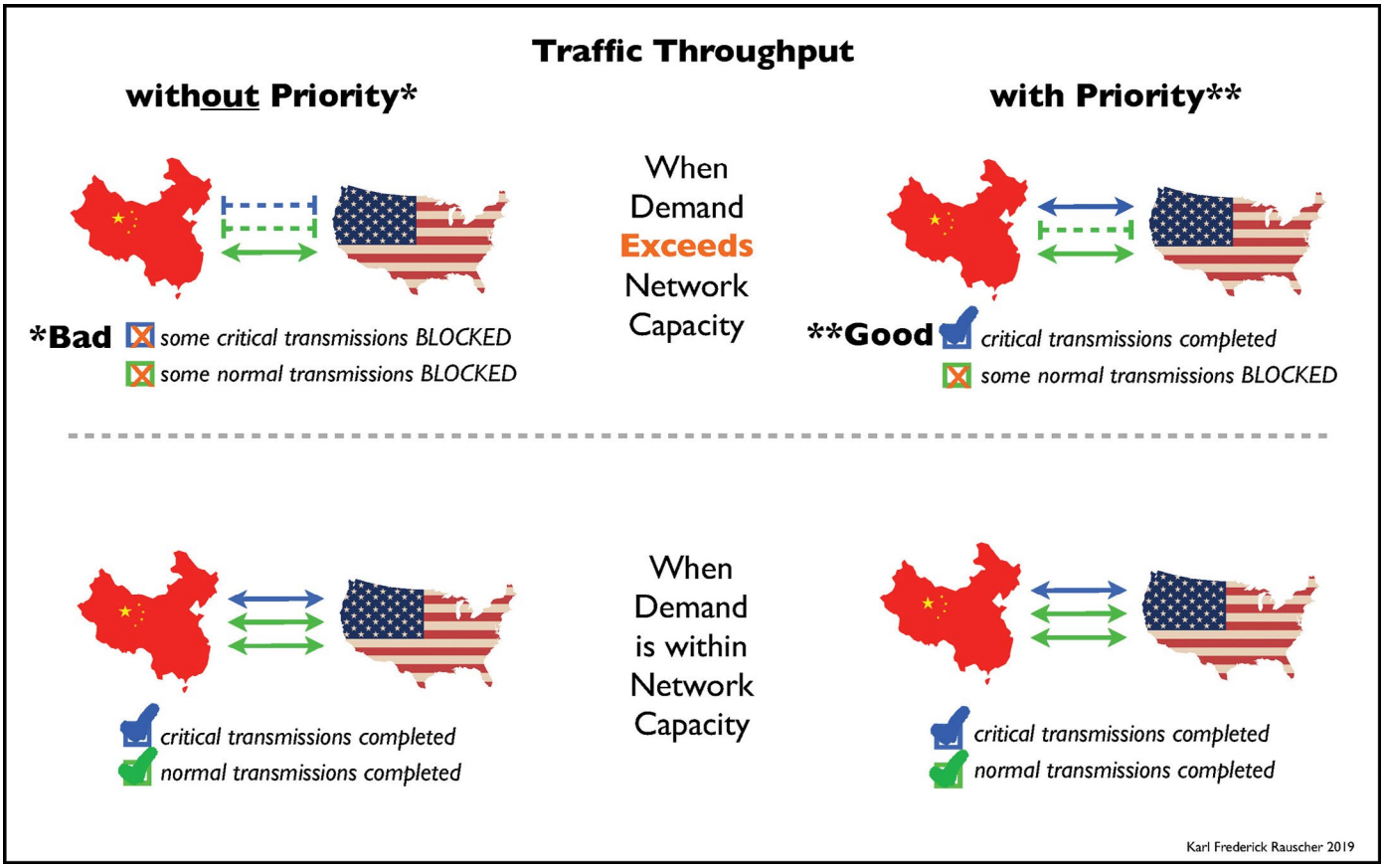


Figure 4. Traffic Throughput without and with Priority.

is more important than others.[48] The end result of this new traffic environment is greater susceptibility to congestion and, thus, to failed communications attempts between both humans and machines. Given the pervasive role of IoT, it is a straightforward conclusion that existing areas of cooperation (e.g., nuclear issues, conflict escalations, economic stability) could be hampered by congestion. If such a communications failure is experienced during a crisis, the consequences could result in significant loss of life and property.

International communications were severely impacted during the aftermath of the 2011 tsunami and Fukushima nuclear accident, the 2010 Haiti earthquake, and the 9/11 terrorist attacks, to name a few examples.[49] DoS attacks are an example of intentional acts designed to exploit the fact that networks have limited capacity. Indeed, IoT devices have already been used to cause distributed denial-of-service (DDoS) attacks, by making use of many devices distributed across many locations so that the source is difficult to pinpoint, isolate, and block. In addition to congestion incidents resulting from extreme natural or manmade events, IoT itself will be the source of congestion incidents. With the huge number of end devices, the range of potential application bandwidth demand, and the constraint of limited network capacity, it is inevitable that congestion will occur. This network-congestion phenomenon has been observed both with the introduction of new technologies with nondeterministic

48 The practice of priority treatment dates back to the beginning of telecommunications. For example, the Pacific Telegraph Act of 1860 gave priority to government messages. Pacific Telegraph Act—An Act to Facilitate Communicates between the Atlantic and Pacific States by Electric Telegraph," Chapter 137, U.S. Statues, 36th Congress, 1st Session, 1860; Myriam Dunn Cavelty and Isabelle Wigert, *International CIIP Handbook 2004: an Inventory of Protection Policies in Fourteen Countries* (Zürich: ETH, Eidgenösse Technische Hochschule = Swiss Federal Institute of Technology, 2004).

49 Other incidents in which traffic congestion impaired critical communications in a crisis include the 2010 Eyjafjallajökull volcano eruption, the 2010 Chile earthquake, the 2009 Australian wildfires, the 2008 Sichuan earthquake, the 2008 Mumbai terrorist attack, the 2008 Russia-Georgia conflict, the 2005 Hurricane Katrina and New Orleans flood, the 2005 London bombings, the 2004 Indian Ocean earthquake and tsunami, the US northeast power blackout, the 2002 floods in China, and the 2002 floods in Europe.

bandwidth utilization (e.g., the first iPhone) and with automated network controls.[50,51] In this sense, IoT network traffic can be thought of as having the potential to cannibalize itself.

In addition to ensuring robust communication (i.e., making sure the most important traffic gets through) during a crisis, a priority scheme is also envisioned, to enhance critical-infrastructure protection. Given the anticipated reliance of every sector on IoT for the operation of critical infrastructure, a priority scheme that ensures robust communications is vital for the safety of human life and the protection of property. While it is not anticipated that the United States or China would deliberately build in reliance on each other regarding the operation of critical infrastructure, some degree of reliance is inevitable in the foreseeable future, given the complexity and international nature of technology supply chains. Both the United States and China should understand not only the specifics and degree of this reliance across each critical infrastructure, but also the role that an international priority scheme could serve, and the additional risks it introduces if used in this application. Given the understandable proclivity of nation states to use technology for a national security advantage, both the United States and China should be cautious about how to proceed in this regard.

To the degree that both the United States and China can implement effective congestion-management schemes in their respective infrastructures, both can have better protection from threats against limited network resources—whether the threat comes from natural, manmade, or even artificial sources, such as the IoT itself.

RECOMMENDATION NO. 2

The US and Chinese governments should agree on a priority scheme for communications traffic across the Internet of Things, to ensure critical US-China communications during a crisis, for both humans and machines.

Required Commitments

The effective implementation of this recommendation will require the following commitments.

- The US and Chinese governments must acknowledge and accept the coming reality of congestion in IoT networks—and its unique nature.
- US and Chinese subject-matter experts must provide expert guidance to their respective governments on suitable congestion-management schemes for IoT, to support international communications for humans and machines.
- The US and Chinese governments must separately establish and implement priority assignment and management systems for IoT, which protect critical infrastructure from foreign attacks and also ensure critical international communications.

Alternatives and Consequences

Alternatives to this approach include the following.

- Do nothing, risking being increasingly unprepared for national emergencies in which increasingly relied-upon IoT services will be unavailable.
- Wait to react until after the first major congestion outage experience takes place, resulting in loss of life and property.
- Rely on industry to solve a problem that it cannot solve without government leadership, allowing for ever greater exposure of human life and property to catastrophic loss.

Benefits

The benefits of implementing this recommendation are enhanced assurance for effective communication during a crisis for existing areas of cooperation (nuclear, international conflicts, economic stability), preparation for new challenges of IoT, and improved robustness against known DDoS attacks. The United States can build upon its proven priority scheme for existing wireline and wireless technologies.[52] The ultimate benefits of this recommendation are the lives saved and property protected.

Next Steps

Suggested next steps to generate and maintain momentum for the implementation of this recommendation include the following.

50 When it was first introduced, 4 percent of iPhone users consumed more than half of the available network bandwidth.

51 Nationwide communications network outage on January 15, 1990. "Peter G. Neumann, Peter, G., *Cause of AT&T NEtwork Failure*, The Risks Digest: Volume 9, Issue 62 - February 26, 1990.

52 Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS).

2-1. The US and Chinese governments separately convene subject-matter experts to determine strategies for IoT congestion management and critical communications, including infrastructure protection.

2-2. The US and Chinese governments, with their respective subject-matter experts, convene to discuss an international scheme for priority communications in the emerging IoT paradigm.

2-3. The US and Chinese governments agree on how critical US–China communications for humans and machines will be prioritized in further IoT rollout.

2-4. US and Chinese businesses implement the agreed-upon plan.

2-5. The US and Chinese governments agree on a schedule and means of periodic testing of the critical communications, and implement this approach.

Measures of Success
The successful implementation of this recommendation can be gauged by the following measures.

A. The United States and China agree to a priority scheme for IoT that provides robust US–China communications during a crisis.

B. US and Chinese critical infrastructures have enhanced protection from DDoS and other attacks.

C. The US and Chinese governments are able to communicate during a crisis in which IoT networks are heavily congested.

D. Businesses are compensated for their initial and ongoing support of the priority scheme.

"It really just showed me how bright he is and how quick he is… And it gave us time together, to kind of learn about each other. He's a lot of fun, and this really brought out really good qualities for him."

MOTHER OF AN AUTISTIC SON SPEAKING AFTER HIS MONTH-LONG INTERACTION WITH A ROBOT[53]

4.3 RECOMMENDATION NO. 3

EXTEND THE ENVELOPE FOR HUMANITARIAN COLLABORATION

Purpose
The purpose of this recommendation is to define a path forward for optimizing the opportunities for mutual benefit to the citizens of both the United States and China regarding IoT applications for human welfare.

Background
IoT has great potential for improving the lives of families. Indeed, the healthcare sector is one of the anticipated early adopters of IoT. With aging populations, the demand for quality healthcare is a major concern for both the United States and China. Growing needs and ever-higher expectations, coupled with the realities of a limited number of healthcare professionals and limited budgets, set the stage for a collision between hopes and reality. The arrival of IoT could not come soon enough for the healthcare sector. The potential for new IoT applications to expand access to higher-quality healthcare is real. As one example of the tangible impact, separate research efforts in the United States and China are making progress in helping families with autistic children via advanced applications of AI and robotics; it is highly likely that collaboration would bring even more benefits more quickly to these families and individuals. Another example is the monitoring of a health crisis in real time, something with which AI and IoT can be well equipped to help. Such

53 Alan Mozes, "Kids with Autism Learn, Grow with the 'Social Robot,'" *Medical Press*, August 22, 2018.

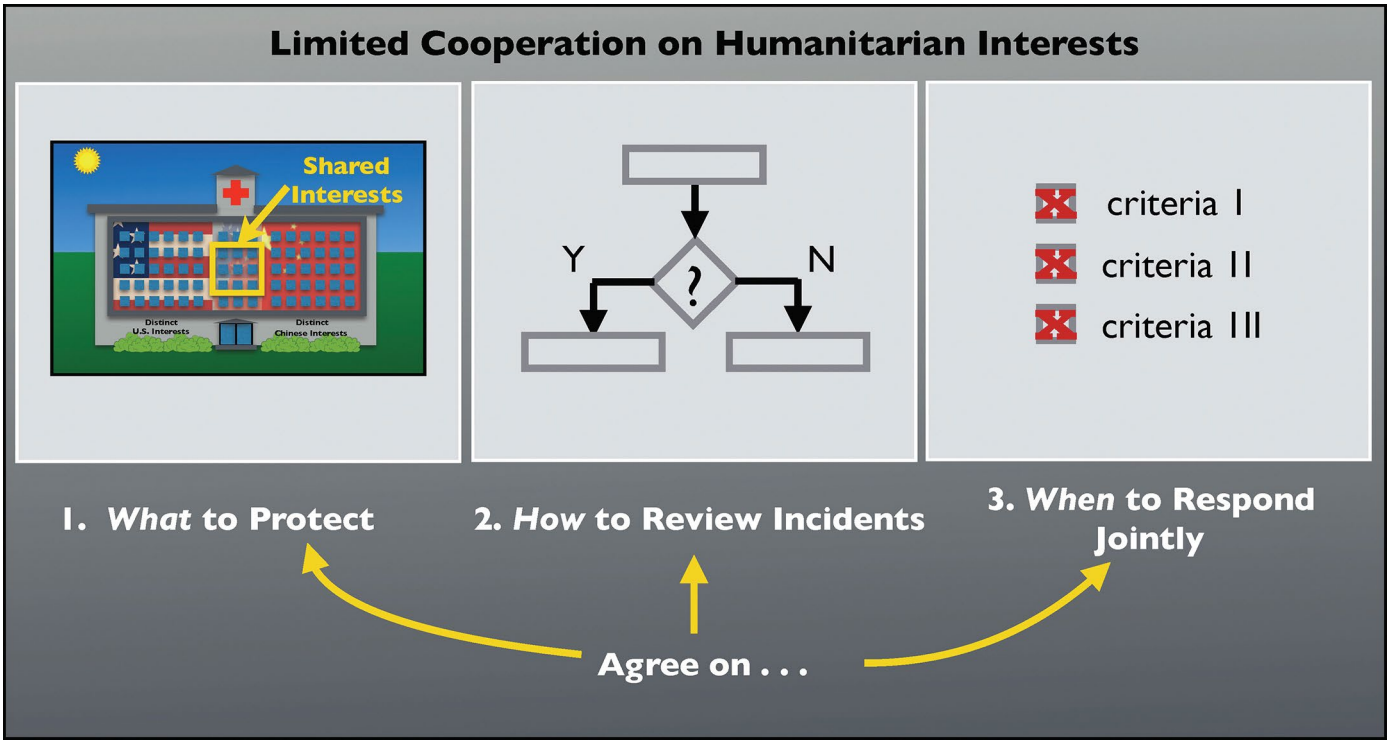


Figure 5. Limited Cooperation on Humanitarian Interests.

collaboration would further extend the lessons learned from the cooperation that took place in response to the SARS epidemic in 2002.[54]

A previous recommendation has called for recognition that humanitarian interests can be distinct from national security and commercial interests. This recommendation extends the envelope of cooperation for humanitarian interests.

In principle, as signatories of international humanitarian law, both the United States and China, as well as many other nation states, already agree that certain human-welfare interests take precedence over the pressing interests and objectives of parties engaged in active military conflict. With the same fundamental values, they should be able to agree that certain humanitarian interests should be protected from other malicious activities. It is reasonable to suggest that both countries can agree on cooperation in three important areas: common ground for what should be protected, a process for how apparent exceptions can be reviewed, and the criteria for when a joint response should be made against offenders.

This recommendation addresses the upside opportunities IoT provides the United States and China for cooperation that can benefit both citizenries, as well as the rest of the world. The recommendation is bold in stating that, in contrast to sometimes-competing national security interests, human-welfare applications of IoT are safe areas of cooperation.

54 *SARS Crisis Jumpstarts U.S.-China Health Cooperation, 2002-2007*, U.S.-China Dialogue on Global Health, Georgetown University, April 2017; Yanzhong Huang, "The SARS Epidemic and its Aftermath in China: a Political Perspective," National Center for Biotechnology Information, National Academy of Sciences, 2004, www.ncbi.nlm.nih.gov/books/NBK92479/.

RECOMMENDATION NO. 3

The US and Chinese governments should cooperate on humanitarian applications of the Internet of Things by establishing policies, providing feedback on the acceptability of each other's policies, collaborating in investigations of incidents noncompliant with stated policies, and confronting parties responsible for causing harm to human-welfare interests in the Internet of Things.

Required Commitments

The effective implementation of this recommendation will require the following commitments.

The US and Chinese governments must agree that some humanitarian interests are distinct from national security interests and deserving of protection in IoT, and cooperate in identifying them.

The US and Chinese governments must seek consensus on how apparent deviations to agreed-upon policies to protect humanitarian interests in IoT should be handled.

The US and Chinese governments must cooperate in seeking some agreement on when a joint response would be warranted to address offenders of protected humanitarian interests in IoT.

Alternatives and Consequences

Alternatives to this approach include the following.

- Reject the notion that humanitarian interests are distinct from national security or commercial interests, leading to overly exposed vulnerabilities in terms of the safety and security of societies that are increasingly reliant on IoT applications.
- Wait for a more formal multilateral treaty-level agreement to be reached, resulting in long delays and missed opportunities to accelerate the development of, and protect the existing applications of, IoT for human welfare.
- Agree in principle, but do nothing, missing opportunities to optimize the benefits of IoT for citizens of both countries.

Benefits

The principal benefit of this recommendation is that it leads the way toward the best-case IoT scenario for citizens of the United States and China, and likely many other places. Other benefits include: accelerated advances in important healthcare fields once the scope of humanitarian interests is mutually defined; the discouraging effect collaboration would have on potential bad actors who would seek to harm humanitarian interest via IoT; and the ongoing processes associated with this recommendation, which would give opportunities for the continued earning and maintaining of mutual trust in broader US-China interactions.

Next Steps

Suggested next steps to generate and maintain momentum for the implementation of this recommendation include the following.

3-1. The US government, Chinese government, and subject-matter experts convene to discuss both the potential opportunities for cooperation in IoT applicants for human welfare and the types of IoT applications that might be candidates for classification as humanitarian.

3-2. The US and Chinese governments agree on an initial, limited scope of humanitarian interests where IoT applications should receive special protections.

3-3. The US and Chinese governments agree on an ongoing forum to identify additional humanitarian interests where IoT applications should receive protections.

3-4. The US and Chinese governments agree on how to handle apparent exceptions to protections of these humanitarian interests.

3-5. The US and Chinese governments agree on when joint action would be taken to address incidents where harm was done to humanitarian IoT applications.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures.

A. New collaboration between US and Chinese scientists and engineers occurs at the intersection of IoT applications and human welfare.

B. The US and Chinese governments agree on a scope of IoT applications for humanitarian interests.

C. The US and Chinese governments cooperate on handling exceptions to policies and addressing malicious actors.

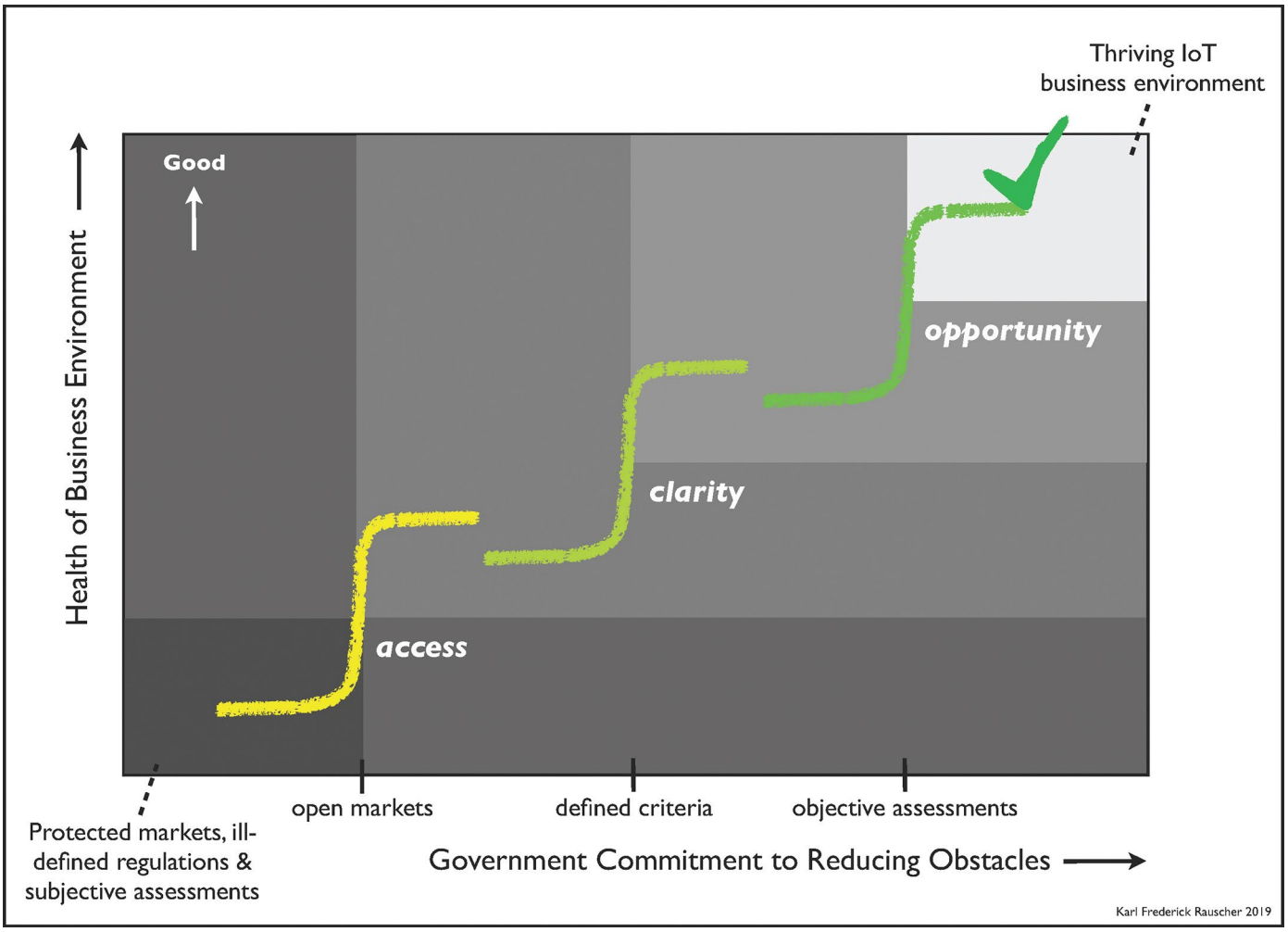


Figure 6. S-Curve Breakthroughs with Open Markets, Defined Criteria, and Objective Assessments.

If you can produce a breakthrough in AI it is worth ten Microsofts.

BILL GATES

4.4 RECOMMENDATION NO. 4

UNLEASH ENTREPRENEURS WITH VERIFIABLE, ACCEPTABLE PRACTICES

Purpose

The purpose of this recommendation is to define a path to a thriving IoT economy grounded in fair trade, and shine a spotlight on the need for clear evaluation criteria for commercial ventures to satisfy the scrutiny necessary to earn trust.

Background

Both the United States and China, as well as many other nation states, see IoT and related technologies as key to economic growth in the coming decade. Both countries would like their businesses to have access to each other's enormous markets and be major players internationally. The opportunities for wealth creation are unprecedented.

From an entrepreneur's perspective, the emerging IoT landscape is full of opportunities. One challenge for entrepreneurs is the obstacles imposed by domestic or foreign governments. Governments are simultaneously anxious about the opportunities to participate in future wealth creation and nervous about the safety and security exposures that accompany the new technology. As a result, governments encourage businesses to

innovate, and simultaneously prepare regulatory measures that may hamper innovation.

These regulatory measures include restrictions on investments, sales, component integration, mergers and acquisitions, and other aspects. Though well intentioned, these regulations are typically problematic for businesses; they are often vague in terms of specifying what is actually acceptable. This lack of specificity is based on the conventional attitude that the technology is too complex and the underlying, fundamental problems cannot be addressed directly. Instead of a knowledge of the intrinsic vulnerabilities that a threat could exercise, historical analogy is unfortunately used as the primary basis of informing and establishing priorities. This is problematic on a number of levels—most notably, in the areas of effectiveness and impedance to economic growth. Regulators typically don't know all the specifics of the problems that they are trying to prevent. Furthermore, there may be procedural reviews that employ subjective judgments. Aside from being suboptimally effective, such processes require time, and introduce uncertainty for businesses whose very survival may depend on winning a race to market.

The recommendation below emphasizes the priorities of businesses, specifically those most likely to take risks to create new wealth across the emerging IoT landscape. Importantly, the recommendation also recognizes that the deployment of IoT exposes national critical infrastructure to increased risks—and, thus, constitutes a national security concern. Indeed, the worst-case scenarios regarding IoT are real possibilities, and could foreseeably involve loss of life and property on a large scale. There is no doubt that governments need to be cautious about the roles foreign businesses are able to assume within their respective realms.

Fear of worst-case scenarios will not halt the deployment of IoT, however, as the benefits of adoption—unprecedented economic, humanitarian, and national security benefits, including enhancements to critical-infrastructure efficiency and reliability—are too compelling. Appropriate due diligence is necessary to address real concerns with this technology. But, how is appropriate due diligence defined?

IoT is, first and foremost, a scientific and engineering arena. Methodologies should therefore be used that acknowledge the bona fide nature of IoT when defining the problem and the solution space. However, having STEM training is not sufficient for an individual to be entirely effective in this arena. Those influencing policy need to master the underlying nature of the technology—an understanding that is comprehensive and a grounding that is systematic. Commanding such a mastery of the problem space is neither easy nor accessible to all, but is possible.

How do the United States and China move forward, knowing the reality that either could exploit IoT intrinsic vulnerabilities to cause serious harm to the other? Do they prefer a world with decreasing trust in the products and services of either country's tech companies, resulting in reduced market opportunities and suboptimal national economic growth? Or, would they prefer a reality in which expanding and merited trust exerts a positive impact on opportunities and growth? Are both of these options viable, and available to pursue?

The more one understands the realities of what IoT will be, the more one is likely to conclude that China is not the biggest source of harm when it comes to IoT and—vice versa—that the United States is not China's biggest source of harm. IoT itself is the most significant agent of expanding exposure to risks. These risks will, in turn, expose national economies, critical infrastructure, and the general public in ways no technology has previously. The collective levels of trust in technology, large technology companies, and AI required for the full adoption of IoT are unprecedented. Consider that young couples will have robots in their homes, often alone in a room with their toddlers. Also, consider that people will soon have a new host of artificial "eyes" watching them, "ears" listening to them, and "brains" constantly analyzing them.

It is not possible for a government to halt the progress of another with regard to their development of IoT. The R&D efforts of a country that is serious about being a player in IoT can greatly benefit from an ocean of readily available information. This is because the entire technology lifecycle is a sieve of information flow. At a minimum, this suggests that both the United States and China need to prepare for a world where both are major influencers of IoT technology.

The following recommendation seeks to seize the economic opportunity, while respecting the daunting security concerns. The recommendation appropriately engages IoT, in that it forces the discussion at the level of accountability—for both businesses and regulators. The recommendation is actionable, in that all of the required commitments are reasonable and preserve national self-interest. The recommendation is bold, in that it replaces the status quo bureaucracy with methods that are more surgical and are informed by the unique nature of IoT.

RECOMMENDATION NO. 4

The US and Chinese governments should, in proportion to the degree each is resolved to encourage the development of a thriving Internet of Things business environment in their respective economies, unleash entrepreneurs by: ensuring fair trade for businesses with IoT products and services; defining the specific acceptable criteria for any trustworthiness requirements for products or services; and providing opportunities for products and services to be verified against the same criteria in an objective process.

Required Commitments

The effective implementation of this recommendation will require the following commitments.

- The US and Chinese governments must decide how important a thriving IoT business environment is to their respective national economies.
- The US and Chinese governments must acknowledge the irreplaceable role that entrepreneurs play in emerging technology businesses.
- The US and Chinese governments must acknowledge the negative correlation between the amount of government regulation and the degree of agility with which entrepreneurs can operate.
- The US and Chinese governments must value the opportunities in each other's markets for their respective businesses, and to their respective national economies.
- The US and Chinese governments must respond to the need to improve vague policies, and effectively articulate what is specifically needed to earn trust and achieve verification.
- The US and Chinese governments must be willing to provide each other with their respective requirements for acceptable policies and verifiable practices to earn and maintain trust in products and services from each other's companies.
- US and Chinese subject-matter experts—qualified with mastery of the underlying scientific principles of IoT—must be willing and available to support their respective governments in developing comprehensive requirements that address the intrinsic vulnerabilities of IoT.

Alternatives and Consequences

Alternatives to this approach include the following.

- Continue a reactive approach by focusing on threats as they occur, resulting in a less-than-acceptable level of control, continued uncertainty about exposure, and wasting limited resources and opportunities to build optimally reliable, safe, and secure IoT.
- Develop and communicate lax requirements for acceptable policies and verifiable practices, exposing either country to exploitation by the other.
- Play political games by expressing a willingness to cooperate but failing to follow through, resulting in confusion for industry, missed opportunities for IoT applications, and reduced access to international markets.
- Do nothing, risking weakened national security, impeded economic growth, and lost opportunities from delays or missed applications of IoT.

Benefits

The benefits of implementing this recommendation are that it optimizes the opportunities for a healthy environment where IoT businesses can thrive via market access and reduced risk. This recommendation also guides stakeholders to better understand and engage with the emerging IoT technology, by requiring that policies be specific regarding exactly what is necessary to earn and maintain trust. This approach defines the appropriate level of due diligence by using a comprehensive and systematic framework for covering each intrinsic vulnerability of IoT systems. Companies will have a lower risk and greater access to each other's markets, and to others around the world. Another benefit is that this approach can be asymmetric—i.e., one country can implement some aspects to a greater extent than the other party, and reap the rewards. Finally, acceptable policies and means of verification can be modified within agreeable timeframes, allowing for flexibility as newcomers arise or lessons are learned.

Next Steps

Suggested next steps to generate and maintain momentum for the implementation of this recommendation include the following.

4-1. The US and Chinese governments engage their respective subject-matter experts to review the landscape of intrinsic vulnerabilities.

4-2. The US and Chinese governments engage their respective subject-matter experts to develop a draft with the specifics of proposed acceptable policies and verifiable practices that would earn and maintain trust, if implemented by the other.

4-3. The US and Chinese governments engage their respective subject-matter experts to review the proposals of their counterparts and provide feedback.

4-4. The US and Chinese governments engage their respective subject-matter experts to assess progress and establish a schedule for the complete implementation of the recommendation. These steps are repeated until an optimal level of trust, given diminishing marginal returns, is achieved.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures.

A. The US and Chinese governments understand and establish their own requirements for trusting each other's IoT products and services.

B. The US and Chinese governments understand the level of verifiable trust that can be achieved, based on specific policies and practices related to exposure to inherent vulnerabilities in their IoT infrastructure.

C. US and Chinese companies have a clear understanding of the design and operational requirements for products and services.

D. The US and Chinese governments each satisfactorily complete verification analyses of areas of concern for each other's practices.

Danger gathers upon our path.

We cannot afford—we have no right—to look back.

We must look forward.

SIR WINSTON CHURCHILL,
PRIME MINISTER OF THE UNITED KINGDOM

5. Conclusion

IoT has the potential to exceed the magnitude of transformation of every industrial revolution that preceded it. Its rollout—which is already under way—is bringing profound changes to society, including very real risks to safety and security at both personal and national levels.

The United States and China, as the world's leading superpowers, have both great exposure to each other's potential to do harm and unparalleled potential to support each other, in addition to other nation states. How these two countries deal with each other on IoT will have truly far-reaching impacts on the world.

At the writing of this report, the United States and China are involved in historic trade negotiations. Whatever the final dispositions of these efforts, questions will need to be answered. To what degree can both countries cooperate on emerging technologies? Are there limited areas of cooperation that preserve the national interests of both countries?

This report anticipates the need to answer these and related questions, and was motivated by the very real national security, commercial, and personal-safety challenges presented by IoT. This document presented eighty-three key observations and a systematic analysis based on rigorous understanding of the underlying scientific principles of IoT. This is not an academic exercise. On the contrary, the report's four recommendations are bold yet sound, actionable yet requiring resolve, and elective yet mandatory to achieve the best possible future. Responsible decision-makers in government, forward-looking leaders in business, and bona fide subject-matter experts across the IoT landscape should urgently move forward with the steps suggested in the preceding pages.

About the Author

Karl Frederick Rauscher is a strategic advisor at the nexus of emerging technology, business and policy. He has served senior business and government leaders on five continents, and is consistently attracted to the challenge of seemingly intractable problems. Karl has over 30 years of business experience in the communications and Internet industry, including 15 years of CXO and board experience with responsibilities spanning profit and loss, cost center and hybrid business models.

While serving as the Chief Technology Officer and Distinguished Fellow of the EastWest Institute, Karl led the first U.S.-China bilateral on cybersecurity with actionable recommendations, Fighting Spam to Build Trust (2011), which he followed up with a second U.S.-China joint report Frank Communications and Sensible Cooperation to Stem Harmful Hacking (2013). He also led the first U.S.-Russia bilateral on cybersecurity with actionable recommendations, Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace (2011), which he followed with Russia-U.S. Bilateral on Cybersecurity - Critical Terminology Foundations, I & II (2011, 2014). Working with the U.S. Federal Reserve, Karl led the first comprehensive study of the world's undersea cable systems that underpin the Internet, i.e. The Reliability of the Global Undersea Communications Cable Infrastructure (ROGUCCI) Report (2010) and led the European Commission-sponsored Availability and Robustness of Electronic Communications Infrastructures (ARECI) (2007).

Previously, Karl was appointed as Vice Chairman of U.S. President George W. Bush's National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Committee. He was elected by industry peers as Vice Chairman of the U.S. Network Reliability Steering Committee (NRSC), was appointed to Chair subcommittees of the U.S. Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) and served on the National Academy of Engineering / National Research Council Critical Infrastructure Roundtable. He is also the Founder and President of the not-for-profit Wireless Emergency Response Team (WERT), which led advanced search and rescue efforts for survivors of the 9-11 terrorist attacks and Hurricane Katrina. He recently served as Ambassador-at-Large and Chief Architect of cyberspace policy at the 400,000+ member Institute of Electrical and Electronics Engineers (IEEE), where he encouraged technologists to engage in critical policy issues that have been created by the digital revolution.

Karl served as Executive Director of the Bell Labs Network Reliability & Security Office and is a Bell Labs Fellow, cited for leading the first achievement of 6 "9's" reliability (99.9999% uptime) of a complex network system and for his role in shaping U.S. homeland security policy for protecting communications infrastructure following the 9-11 terrorist attacks. He has personally discovered over one thousand defects in software running live communications networks and is an inventor with over 40 patents/pending, the first of which was an early breakthrough in artificial intelligence.

Karl serves as Chairman of the strategic advisory boards for Sonavation and CloudMinds, and recently served as a strategic advisory for Liquid Robotics. He is also the Founder of the Association of Cloud robot Operators (ACRO) which was created to facilitate agreements, best practices, standards, and other policy essential to realizing the potential of cloud-connected robots while optimizing the safety and quality of human life. He recently served as an independent Director on the board of Sonavation. Karl serves as a Commissioner, and the Managing Director of the Global Information Infrastructure Commission (GIIC), a federation of chairmen and CEOs affiliated with the world's leading Internet companies with a reach of nearly 200 countries. Media covering his work includes BBC, Bloomberg, China Daily, CNN, C-SPAN, Financial Times, Hindustan Times, The New York Times, PCWorld, Scientific American, Sky News, USA Today, and the Wall Street Journal. Karl holds electrical engineering degrees with high distinction from Pennsylvania State University and Rutgers University, earned a masters in biblical studies with high honors from Dallas Theological Studies, and has completed advanced programs at the MIT Sloan School of Management and the Stanford University Law School Rock Center for Corporate Governance Directors' College.

Appendix A. Application of the Eight-Ingredient Framework to the Internet of Things

A distinct aspect of this report is the methodology used to develop its recommendations. Its insights and subsequent recommendations are based on observations generated from a systematic analysis of the intersection of intrinsic vulnerabilities of the ingredients that make up cyberspace, and trends and other phenomena emerging from the IoT.

As introduced in Section 2.3, Methodology of this Report, the 8i Framework is a proven and powerful structure for comprehensive coverage of the intrinsic vulnerabilities of the eight ingredients that make up cyberspace. Importantly for this analysis, the finite number of intrinsic vulnerabilities for each of the distinct eight ingredients demands attention. Figure 7, 8i Framework Ishikawa Diagram for Network Congestion, provides an example of how a specific problem (in this case, network congestion) is caused. Primarily, the intrinsic vulnerability of networks always having capacity limits and of the payload ingredient having statistical variation and extreme loads results in congestion. Furthermore, intrinsic vulnerabilities of policy, such as outdated and unimplemented standards for handling congestion, unnecessarily allow for a greater impact than is necessary. This example is highly relevant for IoT, as explained in Recommendation No. 2, Priority Scheme for Critical Human and Machine Communications (Section 4.2).

As can be seen in the example below, this analysis is quite detailed. For this reason, the application of the 8i Framework to IoT is left to this high-level description and example. Otherwise, the report would be far too long for the typical reader.

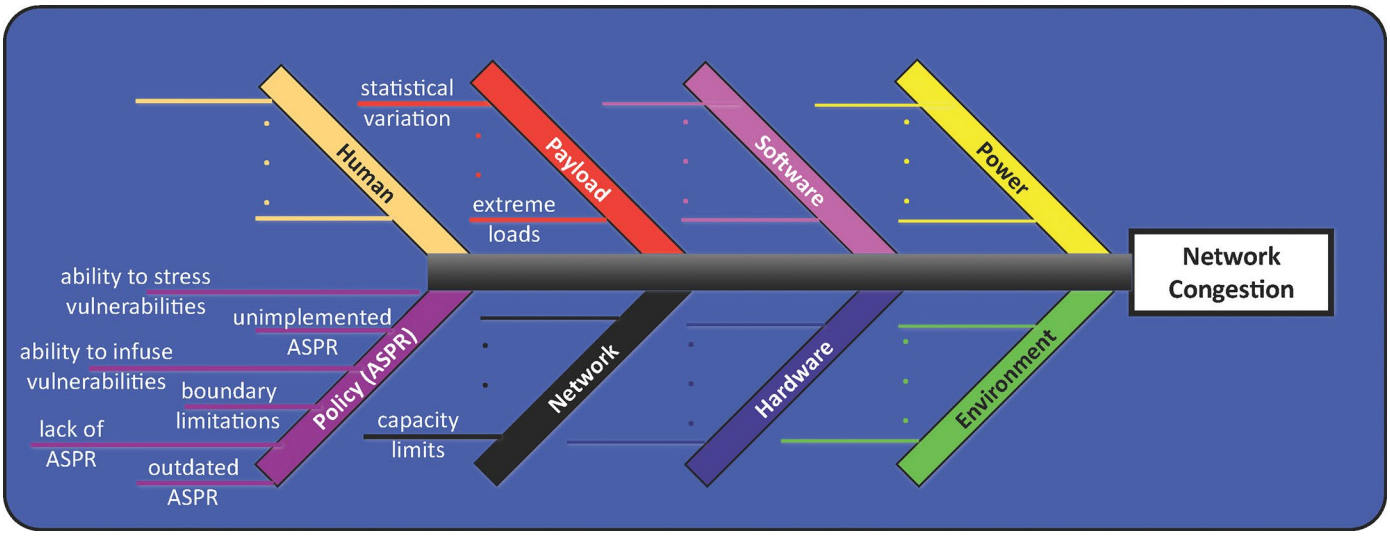


Figure 7. 8i Framework Ishikawa Diagram for Network Congestion.

Atlantic Council Board of Directors

Atlantic Council

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

Atlantic Council

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

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