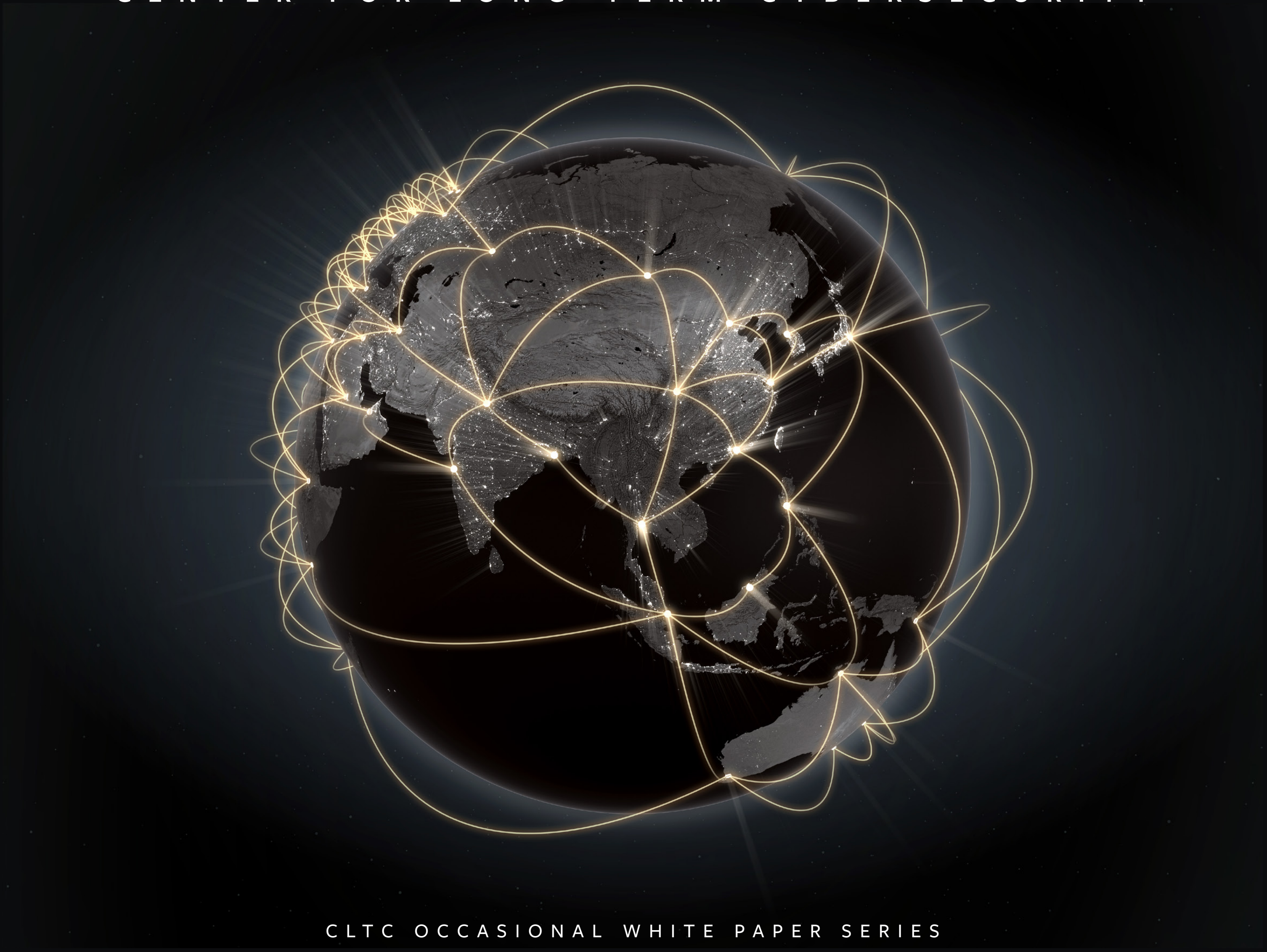
CENTER FOR LONG-TERM CYBERSECURITY



CLTC OCCASIONAL WHITE PAPER SERIES

Asian Cybersecurity Futures

OPPORTUNITY AND RISK IN THE RISING DIGITAL WORLD

JONATHAN REIBER
AND
ARUN MOHAN SUKUMAR

CLTC OCCASIONAL WHITE PAPER SERIES

Asian Cybersecurity Futures

OPPORTUNITY AND RISK IN THE RISING DIGITAL WORLD

JONATHAN REIBER
AND
ARUN MOHAN SUKUMAR

CLTC
Center for Long-Term Cybersecurity

ORF OBSERVER RESEARCH FOUNDATION

CENTER FOR LONG-TERM CYBERSECURITY

Science and technology revolutionize our lives, but memory, tradition and myth frame our response.

—Arthur M. Schlesinger Jr.,
from “The Challenge of Change,” *New York Times*, July 27, 1986

Contents

Executive Summary

Two major geopolitical forces rose in the last generation to change our world. With over 3.7 billion people online as this study goes to print,[1] the internet has melded into our way of life. It reshapes how we do business, how we imagine the world and ourselves, and how we conduct statecraft and warfare. Concurrent with this technological change came another shift in world affairs: the economic rise of the East, led by China and India.

Over the next decade, China and India alone will likely add a billion new internet users. Unlike in the West, however, internet users in Asia are coming online in the uncertain era of cybersecurity and cyberoperations. If ever there was a time when real-world politics and military operations seemed absent from online life, that time has long since past. The forces of internet expansion and rising Asian economic power now converge in a moment of change for which the international system is not prepared.

Given the interconnectedness of the global economy and cybervulnerabilities present in Asia today, the cybersecurity choices that Asian countries and companies make over the next five years will impact millions of lives for a generation. The expansion of the internet in Asia will likely mirror that of the West in some respects, but it will also respond to new risks and opportunities, and evolve within the distinctive Asian political milieu. At this moment of approaching internet expansion, Asians have a unique opportunity to build a more secure and resilient approach to cybersecurity before millions come online.

This study presents strategic choices for Asia's cybersecurity future. It does so by examining scenarios at the intersection of technological disruption and traditional geopolitics. It identifies key premises for cybersecurity in Asia, as well as drivers of change that are likely to shape any cybersecurity future that may unfold. These scenarios explore how diverse forces may interact over time—and point toward options for investment to mitigate risk. The intended audience includes executives, policymakers, researchers, and anyone concerned with the stability and prosperity of the Asia-Pacific.

This study identifies **three cybersecurity premises** that will inform any Asian cybersecurity future. These premises stirred the authors to think about Asia's cybersecurity future and how it may evolve.

1. Asia is largely unprepared for cyberrisks and vulnerable to disruptions, particularly for populations unaccustomed to advanced internet technologies.

2. China's rise will be a dominant force in Asia's future, and the choices that China makes will shape stability and cybersecurity across the region.

3. The novel use of cyberspace operations creates uncertainty in Asia and across the globe, and threatens to exacerbate pre-existing tensions among states and groups.

A range of socio-political drivers of change will impact Asia's cybersecurity future. Key driving questions include:

1. How will income inequality and Asia's rural-urban divide affect cybersecurity, particularly given governmental limitations outside Asia's megacities?

2. In what ways might geography and territorial disputes impact cybersecurity investments and operations?

3. How will nationalism and identity politics evolve as internet access expands? How might nationalist expressions impact cybersecurity?

4. In what ways will Asian cultures shape what was once a largely western technology, and how will they influence the future of cybersecurity?

Asia's cybersecurity story will evolve through the interplay of these forces and others. The question is *how*. Our scenarios offer a prospective look, not to predict the future but to imagine potential storylines and then to highlight gaps and opportunities for change.

1. In **Hack the Farm**, a multinational corporation introduces a new technology into the Indian agricultural sector. A cyberincident disrupts agricultural equipment and draws out tensions among regional capitals, New Delhi, and organized farmers across India's cotton belt. The scenario leads to changes in how diverse Indian and global communities plan for cyberrisks.

2. In **Escalation in the Pacific**, tensions between China, Vietnam, and the United States come to a head in a cyberconflict that results in surprising lethal consequences and unexpected

diplomatic commitments between China and the United States. The story unfolds amidst a backdrop of rising middle-class resistance to the Chinese Communist Party's (CCP) economic policies and online social controls. The events in this scenario alter China's domestic future and the nature of cyberspace operations within the international system.

3. In **The Beijing Cyberconsensus**, China intentionally makes technological investments in four Central and Southeast Asian nations that over time increase Beijing's regional power and shape the region's cybersecurity policies and practices. Absent alternative options, weaker states opt into Beijing's investments and influence, while stronger states, like Australia, India, Japan, and South Korea, opt out.

On the basis of history and an analysis of key trends and drivers of change, these scenarios draw out a number of findings for policymakers and corporate planners, as well as specialists of Asian affairs and cybersecurity. These findings are explored throughout the scenarios and the study.

- **Unlike internet expansion in the West, where access and speed were the first priorities and security was largely an afterthought, Asia can shape its cybersecurity at an earlier stage in its internet growth.** System developers can incorporate cybersecurity technologies into projects now. Public- and private-sector leaders can shape policies and standards and advocate for change. Major markets can influence global companies to improve their cybersecurity practices.

- **At this stage in Asia's internet expansion and economic growth, strategic planning and analysis can have a profound impact on Asia's cybersecurity and economic future.** Rather than adopt a piecemeal approach, strategic planners can look across opportunities and risks to shape the future. Effective strategies can help strengthen relationships across sectors, prepare for cyberattacks of significant consequence, and identify gaps in developing cybersecurity capabilities.

- **The scope of the problem demands that Asian organizations plan to perform missions and functions without assured access to secure data.** In rising digital Asia, it is not a question of if but when cyberattacks and disruptions will occur. As the internet expands and populations become increasingly dependent upon it, societies must focus on resilience to withstand data disruptions and manipulations of critical infrastructure (i.e., of the finance, energy, and national security sectors), and also to withstand cyberinfluence

> operations of online media that could alter political perceptions. The scenarios outlined in this report suggest pathways for achieving resilience in society at the technological and political levels.

Much is at stake as Asia rises economically and militarily and as millions of internet users come online. The internet has shaped Asia over the last decade, but it is about to spike in its influence as access expands dramatically in the world's most important economic region. The study provides a framework and invites readers to think further about the region's technological, political, and cybersecurity future.

Acknowledgements

This study would not have been produced or developed without the gracious support of a number of individuals and organizations. The authors wish to thank Steve Weber, Faculty Director of the UC Berkeley Center for Long-Term Cybersecurity, and Samir Saran, Vice President, Observer Research Foundation, for supporting the vision and concept of this study and for providing funding and analytic thinking to shape its development. Shazeda Ahmed, Arindrajit Basu, and Madhulika Srikumar provided excellent research support in the early part of the project's development. The Center for Long-Term Cybersecurity's Chuck Kapelke and Betsy Cooper provided valuable editorial recommendations and copyediting, and Nicole Hayward helpfully designed the final product.

Scenarios are best considered through conversation, and the authors wish to thank a number of individuals for their comment and review of the document, including Chinmayi Arun (National Law University, New Delhi), Patrick Cronin (Center for a New American Security), Richard Danzig (Johns Hopkins Applied Physics Laboratories), Jesse Goldhammer (UC Berkeley School of Information), Jim Miller (Belfer Center for Science and International Affairs), Daniel Melleby, James Mulvenon (Hoover Institution), Jennifer Staats (U.S. Institute of Peace), Vinh Nguyen, and Lucas Klein (University of Hong Kong), all of whom read versions of some or all of the report. A number of senior government officials also reviewed the report, and we are grateful to them. Shivshankar Menon (Brookings Institution), Ron Deibert (Citizen Lab), and Adam Segal (Council on Foreign Relations) offered early assistance in thinking about the future of cybersecurity in the region. Diveena Cooppan provided remarkable support as a reader and editor. Finally, the authors wish to thank Eli Sugarman and the team at the Hewlett Foundation for their support to the Center for Long-Term Cybersecurity and the Observer Research Foundation. Without Eli's support, none of this work would have been possible.

The authors are grateful to all who contributed to this report's review and development; any errors or inconsistencies, of course, are wholly our responsibility.

Jonathan Reiber,
Berkeley, California

Arun Mohan Sukumar,
New Delhi, India

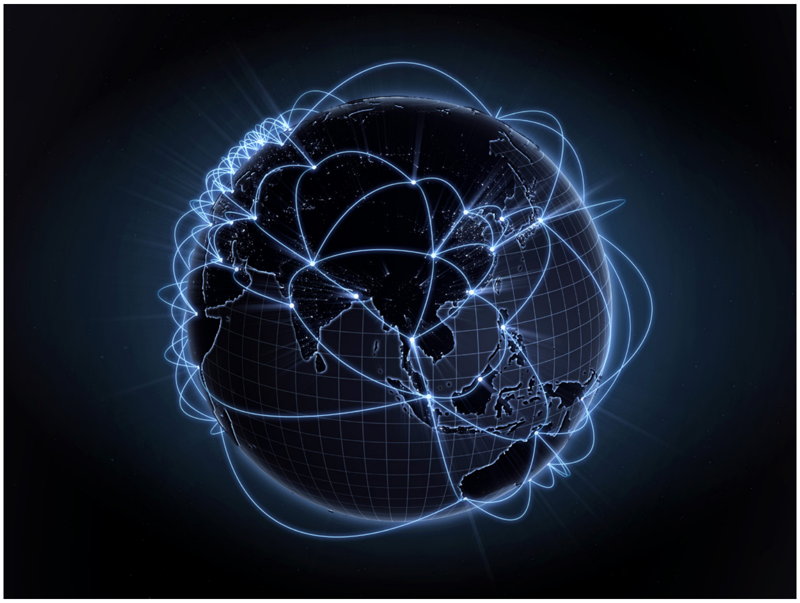
THREE SCENARIOS SUMMARIES

1. **Hack the Farm.** With the widespread use of Unmanned Aerial Vehicles (UAVs) as crop-dusters and sprayers in India's cotton belt, agricultural productivity is set to rise manifold. A sophisticated malicious tool, disguised as a patch to the GPS system of the Yamaha "R-Max 2" drone, wreaks havoc on the cotton fields, destroying a season's output and triggering a political crisis in India. The Indian national government and state governments work together and with multinational companies to improve India's cybersecurity posture, but not without costs.

2. **Escalation in the Pacific.** In the face of an economic downturn, China struggles to shore up its energy resources in the South China Sea,[2] and, through an escalatory action, triggers a Vietnamese cyberattack on Chinese assets. An inadvertent Chinese cyberattack then destroys data at a Vietnamese hospital, killing four people, including two American citizens, in the first known deaths due to cyberweapon usage against civil infrastructure. The United States, Vietnam, and states in the Association of Southeast Asian Nations (ASEAN) are drawn into a moment of cyberspace conflict escalation with China that changes China's future and that of the world in surprising ways.

3. **The Beijing Cyberconsensus.** Four Central and Southeast Asian countries—Tajikistan, Kyrgyzstan, Laos, and Cambodia—have yet to articulate robust cybersecurity standards for their countries. In this scenario, all four countries win assistance from the Asian Infrastructure Investment Bank (AIIB) to overhaul and strengthen their lagging information communications and technology (ICT) infrastructure. The bids to perform these contracts—from the setting up of telecommunications towers, to the subsidized sale of handheld devices—are all won by Chinese ICT companies. The Chinese firms' influence over Asia's ICT systems ultimately molds cybersecurity policies favorable to Beijing. Some countries opt in, some opt out, while others try to push back on China. The scenario raises a range of questions for ICT owners and operators, citizens, and policy planners in thinking about China's and Asia's future.

Introduction



Today Asia is a vibrant center of the world economy. Mumbai, Hong Kong, and Shanghai play as important a part in the global order as London, New York, and Tokyo did thirty years ago. Under current trajectories, the U.S. National Intelligence Council anticipates that Asia will surge past North America and Europe in influence by 2030, thanks to its population size, gross domestic product (GDP), military spending, and technological investment.[3] By then, China will have the world's largest GDP; it is already the largest economy in the world by purchasing power parity, followed by the United States and two other Asian nations: India and Japan.[4] Such a geostrategic change carries significant implications for world affairs, particularly at the nexus of politics and technology. This study explores the future of cybersecurity in Asia as the region rises and its political and technological influence expands.

The internet has played a major role in Asia's rise. Telecommunications investments in China, India, and Southeast Asia intensified the integration of Asian economies into the global economic system over the last three decades and allowed Asian companies to bring goods and services to domestic and international markets in new ways.[5] On the back of telecommunications investments, mobile and e-commerce platforms proliferated; internet-based services like China's Didi Chuxing and Alibaba, India's Olacabs and Flipkart, and Singapore's GrabTaxi are now some of the world's most highly valued companies.[6]

This is likely just the beginning of Asia's internet-enabled economic growth. At the end of 2016, China had the largest population of internet users on earth at 720 million, and India jumped past the United States for second place with over 460 million users.[7] Yet outside of South Korea, Japan, Singapore, New Zealand, and Australia, much of the Asia-Pacific has yet to come online. Compared to the United States, which hovered at just below 90% user penetration at the end of 2016, China and India had only 51% and 36% penetration respectively; Vietnam, the Philippines, and Thailand were at or just below 50% each.[8] If China and India alone were to achieve 90% penetration, this would add more than a billion new Asian users to the global internet population.

Asia will likely add at least a billion new internet users in the coming decade

This projected growth presents a remarkable statistical change in the shape of the internet: it took over thirty years for the first 3.7 billion internet users to come online. Since Facebook's founding in 2006, the company claims that it has added two billion monthly users.[9] Asia will likely add at least one third of today's total population in the coming decade alone, and we are still coming to grips with how increased access to internet technologies change our world, from echo chambers to destructive cyberattacks.

Unlike the West, Asia rises amidst the information revolution. We live in a world economy that is defined more by data management and intellectual capital than traditional forms of agriculture and manufacturing. Asian leaders know they must build a knowledge-based economy if their populations are to compete and continue their transition toward middle-income status. Political leaders across the region thus have invested in initiatives to digitize their economies, from Digital India to Singapore's Smart Nation Initiative.[10] But have they prepared for the political and security impacts of the internet?

Unlike the West, Asia rises amidst the information revolution.

Cyberspace operations and cyberattacks present a dark side to this surge of internet connectivity. The history of the last decade shows how the internet can be used as a tool of domestic and international conflict, from the internet-enabled democratic uprisings in the Arab World to the conduct of cyberspace operations to manipulate data, as in Iran's 2011–2012 distributed denial of service attacks on the U.S. financial sector,[11] or Russia's cyber-enabled influence operations to tip the outcome of the 2016 U.S. presidential election in favor of Donald J. Trump.[12] If ever the world assumed that the internet could exist in a space outside of politics, that time of innocence has passed. Millions of Asians will come online at a time when the world has already learned to use the internet as a tool for domestic politics and military operations. Asian political forces, from class struggles to great power rivalries, will express themselves in cyberspace as Asia rises, pushing up against forces within Asian countries and the broader world. Old worlds will meet new technologies, likely increasing the potential for social and political disruption and change.

The future of Asia's cybersecurity will carry worldwide implications. China, Japan, South Korea, and India rank among the United States' top ten trading partners.[13] Disruptions to Asian assets have the potential to entangle the United States, as demonstrated by the 2016 cybertheft of $101 million dollars from the Bangladesh Central Bank account at the New York Fed Reserve.[14] Globalization knits the world economy together, and a disruption of Asian-based shipping, banking, and manufacturing data could easily affect other countries. In addition to economic risks, the United States has a significant forward military presence across Asia as part of the U.S. rebalance to the region, with forces in Japan, South Korea, Singapore, and Australia, among other countries.[15] Asian cybersecurity matters not just for Asia, but also for U.S. national and economic security, for the functioning global economy, and for alliance operations, particularly if the critical infrastructure that supports regional militaries is ever disrupted.

This study explores how Asian cybersecurity might evolve over time. We focus particularly on China, India, and the United States—the states with the greatest political and economic influence on Asia's strategic future and the largest numbers of current and projected internet users. Asia stands at a unique moment before internet access expands; countries have an opportunity to make a range of strategic choices to shape the region's future. The emergence of China as a political power in particular will shape any cybersecurity future that may unfold. Traditional political stories will play themselves out in new and unfamiliar ways as the internet expands. Activists will protest on the streets and online. States will threaten each other's centers of gravity through cyberspace.

> Asia stands at a unique moment before internet access expands; countries have an opportunity to make a range of strategic choices to shape the region's future.

Some key questions can spur and frame our thinking. How will Asian governments manage a future where digital technology touches the lives of lower–income and rural populations? How will less technologically developed sectors, like the agricultural sector, evolve as advanced technologies enter Asian markets? As China rises, how will great powers interact across the Pacific during periods of escalating hostilities, and what issues may be exacerbated or resolved through the use of cyberpower? Regionally, what will China's economic dominance mean for technology and the growth of the internet across Asia? Ultimately, how can Asian governments and companies best seize this moment of opportunity presented by expanding access? By looking at how key drivers of change would interact with actors and institutions across the region, scenarios help us imagine how the future may unfold.

WHY SCENARIOS?

Organizations have long used scenarios as a part of their strategic planning. The practice of scenario thinking became more popular in the private sector after Royal Dutch Shell claimed better foresight into the oil crisis in 1970s, a geopolitical surprise that caught most other oil companies and analysts by surprise.[16] Now scenario planning is widely used. Governments have put the practice to use: the U.S. National Intelligence Council's "Global Trends" report[17] imagines future trends that could impact policy, and produces smaller scenario projects for the government if requested by policymakers. The U.S. Defense Department uses an array of classified scenarios and exercises to anticipate and prepare for potential conflicts and make investments.[18]

Scenario planning typically considers diverse "drivers of change"—key forces active in a society—and explores how they could interact with actors, institutions, and populations to alter the trajectory of the future. Scenarios help inform policy and corporate strategic planning and academic research by providing three main benefits, each of which applies as we think about Asia:

1. *Scenarios help us step away from the tactical world.* Scenarios stretch the minds of strategists, planners, and investors to think beyond conventional wisdom. Exploring the intersection of key drivers and actors in a scenario narrative can help identify a range of potential future events, which may provoke planners or investors to rethink their underlying assumptions about the societies in which they operate and the tools they have available to effect change.

2. *Scenarios help us see beyond our area of expertise.* Cybersecurity experts may see the world from their own particular lens of cyberspace operations, market forces, or technolo-

gy development. The best scenarios examine broader forces at work in societies, from political narratives and ideology to class behaviors to the development of commercial industries that haven't traditionally associated with information technology, like the agricultural sector. In this way, scenarios help experts see the security implications of broader trends.

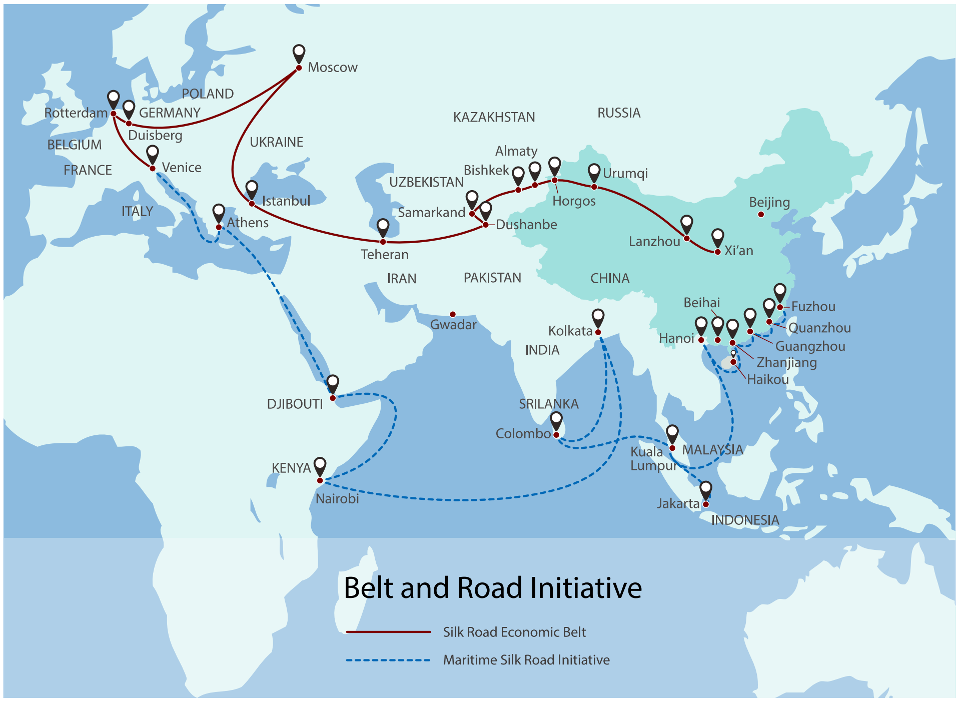
3. *Scenarios highlight the value of resilience and can suggest paths for achieving it in the face of unexpected events.* Scenarios can help policy planners, investors, and technologists discover new areas of inquiry to shape the future world. Sometimes such analysis helps with future shocks. For example, in a famous scenario-based planning exercise, a global delivery company contracted a consulting firm to help prepare for the potential impact of avian flu on its global operations. The firm analyzed the company's global logistics chain to see how a flu outbreak could have an impact, and then proposed a series of resiliency plans to mitigate risk. The avian flu never affected the company's operations, but something else did: In the summer of 2010, Iceland's Eyjafjallajökull volcano erupted and spread ash all over northern Europe, disrupting flight paths for weeks. Commercial airlines lost millions of dollars. Since the company had already imagined how it would respond to a disruption, however, it was able to continue its operations when others were not. Scenarios raise potential issues for exploration and can ultimately help mitigate risk when unforeseen events occur.[19]

In 2016, the University of California, Berkeley's Center for Long-Term Cybersecurity produced *Cybersecurity Futures 2020*, a set of five scenarios that explored long-term trends in cybersecurity, the internet, and data management.[20] Following the publication of that report, Arun Mohan Sukumar of the Observer Research Foundation in India proposed the development of a set of scenarios focused on the Asia-Pacific region for the 2016 CyFy conference in New Delhi. This study emerged from that idea.

These scenarios are not meant to be predictive; confident predictions are not a good basis for planning.[21] Scenarios are intended instead as a tool for organizing thinking and imagining potential futures. They can help policymakers better imagine strategic options available to them, and build capabilities to respond to an inherently unpredictable international system.

THREE CYBERSECURITY PREMISES

In the era of Asia's internet growth and rising political power, three premises combine to make cybersecurity a vital factor in Asia's future. They set the cybersecurity stage and provide context for interpreting the scenarios and understanding why and how certain narratives may



unfold in the region. From within this context, decision-makers can read the scenarios to see how premises may interact with key drivers of change to alter the future.

1. In a world where cyberdependence already exceeds cybersecurity, Asia's cybersecurity practices lag behind those of other regions. Computer code is vulnerable to exploitation and attack globally, and Asian countries and companies are largely unprepared for the cyberrisks they may face, whether from data-manipulative attacks like that which Russia reportedly conducted against Ukraine's electric grid in the winter of 2016, to criminal activity like the 2016 hack of the Bangladesh Central Bank. A yearlong study by Mandiant (a cybersecurity firm now owned by parent company FireEye) found that Asian-based companies rank poorly in following global cybersecurity best practices; they frequently lack the expertise, threat intelligence, and technological systems required to prevent, detect, and respond to intrusions and cyberattacks. For example, Mandiant reports that Asian companies took an average of 520 days between a breach and its identification, compared to 146 days as a worldwide average.[22]

In addition to the Mandiant report, in a 2014 white paper on Asian defense spending the consulting firm Deloitte found that, within Asia, the more developed and internet-penetrated Asian economies remain the most vulnerable to disruptions in the short term. Deloitte found that South Korea, Australia, New Zealand, Japan, and Singapore were nine times more vulnerable to cyberattack than the other thirteen Asia-Pacific economies, and that "South Korea's rapid move toward ubiquitous wireless access propelled it to the highest score for cyberrisk in 2014." Over the long-term, however, Deloitte anticipated that the more populous and less developed countries of China and India will become more vulnerable to attacks as internet access expands across sectors.[23]

The growth of the cybersecurity sector is good news for those with sufficient resources and established institutional structures to protect themselves, like South Korea, Australia, New Zealand, Japan, and Singapore. Yet growth in the cybersecurity market alone will not help to manage political risks exposed by broader socio-economic forces, such as class tensions and the growing gap in technology skills in China and India and other states. Meeting Asian cybersecurity challenges requires partnerships across sectors, and scenarios can help readers identify gaps and specific solutions.

2. China's economic and military rise leaves Asian states uncertain about the region's stability and their own security. China's significant strategic investments (including in military forces focused on cyberspace operations), the lack of a robust regional security architecture (like NATO) to counter China's activities,[24] and Chinese assertiveness in the South China Sea and elsewhere all contribute to a sense of collective unease.

In 2011, China's political and military assertiveness, coupled with the growing importance of Asia to the global economic order, spurred the United States to begin a diplomatic, economic, and military "rebalance to Asia" to maintain peace and stability and ensure economic prosperity in the region.[25] A peaceful and productive U.S.-China relationship is central to the future health and stability of the Asia-Pacific region, and cybersecurity figures prominently in the two countries' dialogue.[26] The prospects of China using its economic clout to re-engineer cyberspace regimes across Asia—or create new regimes altogether—is a cause for concern, as the contours of Beijing's strategic intentions remain unclear.[27] This is particularly the case regarding China's "Belt and Road" initiative, a major economic investment initiative of Chinese President Xi Jinping that seeks to extend Chinese trade as well as foreign policy and economic influence across Eurasia.[28] The Belt and Road Initiative also includes significant information and communications technologies investments; these and other material investments all contribute to a sense of unease surrounding China's rise.

3. Compounding the first and second trends, the novel use of cyberspace as a strategic tool for military and intelligence operations by state and non-state groups can exacerbate pre-existing geopolitical tensions. States around the world have pushed the outer edge in exploring how to use cyberspace to achieve their political and strategic objectives. They have penetrated each other's critical infrastructure[29] through cybertools, destroyed data to suppress content distribution, and conducted financial theft, often breaking new ground in achieving specific cyber-enabled effects. It seems that with each passing week the world learns about a new kind

of digital manipulation. As global cyberthreats have increased in severity and sophistication, Asian states have designed cyberstrategies and invested in cybercapabilities for defensive and offensive purposes: Australia, China, South Korea, and Japan are the most advanced and organized actors in the Asia-Pacific, mirroring their broader military and economic development,[30] while North Korea has displayed overt hostile intent in cyberspace through the repeated use of destructive cyberattacks on South Korea, the United States, and others.

States have responded to cyberattacks or intrusions through actions and words to clarify what is acceptable and what is not, and have begun to set norms of behavior in cyberspace. Yet there is still a significant degree of uncertainty regarding norms and governance of cyberspace operations. One factor that underpins this problem and exacerbates uncertainty is that states have not agreed on the nature of international law in governing cyberspace operations, nor have they agreed on specific proscriptions regarding targets that should be off-limits during hostilities. The United States, for example, has consistently argued that the Law of Armed Conflict applies for governing cyberspace operations just as in other domains of military operations.[31] China has demurred on committing to the Law of Armed Conflict, and instead offers alternative governing concepts. For instance, China supports a Shanghai Cooperation Organization (SCO)-driven "International Code of Conduct for Information Security"[32] that indicates the potential for China's increased control over aspects of the internet. China may have differing perspectives regarding the applicability of laws of self-defense and limits on cyberspace operations, including proportionality of response and operations (reconnaissance or otherwise) against civil targets, actions that could lead to perceptions of escalating cyberconflict, and potentially a crisis in interstate relations. Some progress has been made through the Group of Seven and in non-binding United Nations norms, but a lack of bilateral or multilateral binding agreements with China on operations leaves the door open for miscommunication and potential escalation.

This trifecta combination of increased vulnerability, uneasiness caused by China's political and military rise, and uncertainty surrounding the use of cyberspace operations makes cybersecurity a vital issue for Asia's present and future.

HISTORICAL CONTEXT: CYBERSPACE OPERATIONS AND CYBERDETERRENCE

If the past is prologue for Asia's future, recent history indicates that the cyberthreat is increasing; historical examples of state behavior in cyberspace can help readers imagine how state and non-state actors might conduct cyberspace operations in Asia in the future—and also help policy planners think about how best to deter and respond to potential cyberattacks.

Cyberspace gives weaker players a sling to launch stones at giants, as demonstrated for instance by Iran's targeting of the United States' financial sector (according to the U.S. Department of Justice) through distributed denial of service attacks in response to economic sanctions.[33] It also gives strong states a stick with which to attack weaker ones, as with Russia's reported distributed denial of service attacks on Estonia's internet infrastructure in 2007 that cut the country off from global internet communications.[34] Cyberspace provides a wide range of potential strategic uses; below are illustrative examples, variants of which could play out in the future in Asia or other regions. State or non-state groups may seek to:

1. *Manipulate or steal data for economic espionage, economic warfare, or financial gain.* A state or non-state actor can hack into a firm to manipulate its internal financial data for a variety of reasons, from undervaluing the firm to stealing intellectual property. According to the U.S. government, the People's Liberation Army (PLA) of China has stolen American intellectual property to benefit Chinese companies; in one instance, the U.S. Attorney of Western Pennsylvania indicted five members of the PLA as reprisal in 2014.[35] The 2016 hack of the Bangladesh Central Bank assets held at the U.S Federal Reserve in New York may also fall into the category of economic theft.[36]

2. *Conduct undeclared disruptive cyberspace operations that fall below the level of conflict to send a message.* The cyberattacks on Sony Pictures Entertainment, attributed by the U.S. government in 2014 to North Korea, may fall into this category. In this case, hackers destroyed data and released emails from Sony Pictures Entertainment in retaliation for its planned release of a satirical film depicting a fictionalized assassination of North Korean leader Kim Jong Un. In response to the North Korea attack, President Barack Obama delivered a statement in December 2014 that the United States would respond proportionally and "in a place and time and manner that we choose."[37] The United States then deployed further economic sanctions against the North Korean regime. Another example of a disruptive cyberspace operation was Russia's reported malware attack on Ukraine's electric grid in December 2015, which shut off electricity for 225,000 Ukrainians for up to six hours across all affected areas,[38] and another attack a year later on the electric grid in Kiev.[39] These attacks may have been intended to rattle Ukraine's resolve or for Russia to demonstrate how it could use cyberweapons against Ukraine, the United States, or others.

3. *Conduct a covert cyber-physical destructive attack below the level of conflict.* According to open-source reporting, between 2008 and 2010 a cyberspace actor deployed the Stuxnet virus against the controls of Iranian nuclear centrifuges with the intent to slow Iran's development of a nuclear weapon capability. The attack, which so far has not been formally attributed to any party, was the first known successful disruptive cyberattack on a cyber-physical industrial system to achieve a significant strategic effect. It altered the landscape of international security affairs.[40]

4. *Conduct influence operations to alter political perceptions and outcomes.* According to the U.S. intelligence community, Russia "conducted a coordinated influence campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency." In addition, "Putin and the Russian Government aspired to help President-elect Trump's election chances when possible."[41] The operation left the world with the impression that states can use cyberspace operations to alter the outcome of another state's political future.[42] In an early response to the Russian hack, the United States sanctioned the Russian regime and expelled Russian government personnel.[43]

5. *Conduct a massive destructive cyber-physical attack of significant consequence to cause a mass loss of life or significantly disrupt the functioning of a society's critical infrastructure to impact a large portion of the population*, whether by shutting off logistics, terminating power systems, or destroying the data that powers a state's infrastructure. (As opposed to the niche focus of the Stuxnet case, such an attack would focus on population-centric effects.) The closest the world has come to seeing such an attack to date is probably Russia's cyberattacks on the Ukrainian electric grid in 2015 and 2016, yet no loss of life was reported in those instances. While a major, population-centric, nationally disruptive attack on critical infrastructure has not yet occurred, preparing to deter, stop, or recover from such an attack is a prevailing concern for the national security community, particularly in more developed and networked economies, where critical infrastructure systems are especially vulnerable to exploitation by cyberattack.

In responding to cyberattacks, including some of those listed above, states and corporations have taken a range of defensive actions, from bolstering internal network defenses (as in Saudi Arabia's response to a malware attack on its oil conglomerate, Saudi ARAMCO),[44] to more deterrence-focused governmental responses, as when the United States imposed sanctions and expelled Russian governmental personnel following Russia's cyberspace operation against the 2016 U.S. presidential election.

In the simplest terms, deterrence is a function of perception that works by convincing a potential adversary that the costs of conducting an attack would outweigh any potential benefits. States can alter a potential adversary's cost-benefit analysis through a combination of (1) preventing a potential attack from succeeding by enhancing cyberdefenses; (2) imposing costs on a potential attacker through cyber or other means; and (3) building resilience to withstand an attack.[45] To succeed, theoretically, each action should raise the "cost" imposed on an opposing actor either by making it harder for the attack to succeed or by imposing punishment for the action.

Deterrence and response options require effective attribution of an attacker's identity to build legitimacy, as well as some communication by leaders regarding the unacceptability of an action. For example, since 2010, U.S. government officials have regularly made what are called "declaratory policy" statements about U.S. response options, signaling that were an adversary to cross a certain threshold in a cyberattack—a threshold determined on a case-by-case basis by the U.S. national security team and the president[46]—the U.S. would respond as needed, including potentially through kinetic military options. Over time, such statements and responses set precedents for acceptable behavior; setting clear norms for what is acceptable and what is not acceptable from a policy, legal, and operational standpoint remains a key part of the evolving cybersecurity and deterrence landscape.

These historical examples provide context for thinking through decisions and events within the following scenarios. Rather than looking at cyberspace operations myopically, however, the scenarios examine incidents and attacks from within the broader geopolitical and management context of dynamism and change in the region. Given the cybervulnerabilities in Asia and projected internet access expansion in the region, what are some of the key political and socio-economic forces that will shape the future of cybersecurity as Asia rises?

POLITICAL AND SOCIO-ECONOMIC DRIVERS OF CHANGE

A range of political and socio-economic drivers of change will shape Asia's technological and cybersecurity future. These drivers of change could include income inequality, particularly across the rural-urban divide, that could drive tensions between those with access to technological opportunities and those without, and the related issue of limits on developing states' governmental institutional power to affect change on a national level; geographic realities, including long-standing territorial disputes that may contribute to inter-state tensions and economic behaviors between dominant and lesser centers of power; and nationalist narratives that may rise in the face of political and technological change at the state and sub-state level. How and why might these drivers play out in the future in Asia?

- *Income inequality and the rural-urban divide.* Although the Asia-Pacific region has risen economically, much of that rise has happened along the industrial spine of the Asia-Pacific's megacities. This is due in part to the relative weakness of Asian state institutions in fostering wealth and providing education to areas outside of major urban environments, a global problem that is particularly acute in developing Asian states. Technological change, globalization, and market reform have brought wealth to millions while many have been left behind.[47] In a number of elections over the last generation, rural voters have rejected ruling parties when technocratic policies have failed to extend benefits beyond the limits of major

urban areas.[48] Asian governments seek to bring mobility and internet access to rural environments, but success is by no means guaranteed.[49] Nor is political stability: As we've seen in the United States and Europe, in the event of socio-political disruptions like an economic recession, access to technology can enable nationalist and reactionary movements and exacerbate tensions as groups harden their opinions and organize online.[50] The scenarios **Hack the Farm** and **Escalation in the Pacific** both explore issues regarding the interaction of technology and class divisions in societies in transition.

- *The power of geography, from territorial disputes to regional economic domination.* Border disputes can become trigger points during heightened tensions, as World War I and more recent history have shown. The Asia-Pacific region contains a number of unresolved territorial disputes between powers, from regional disputes over the South China Sea to conflicts over Jammu and Kashmir along the Indo-Pakistan border[51] to the Demilitarized Zone between North and South Korea, to lesser disputes like those between China and India over Aksai Chin, the Doka La crossing,[52] and Arunchal Pradesh[53] and between Japan and China over the Senkaku/Diaoyu Islands.[54] Tensions could lead to actions taken in physical spaces as well as cyberspace.

  Beyond territorial disputes, great and regional powers consistently use their economic and political advantages to influence states on the geographic periphery that are dependent on their economic power.[55] Technology can play a role in overt or subtle modes of domination, as dominant powers may seek to manipulate lesser powers in their "near abroad" in an effort to achieve economic expansion. **The Beijing Cyberconsensus** focuses on this dynamic, while **Escalation in the Pacific** explores the potential nexus of territorial disputes and cyberspace operations.

- *Nationalism or identity politics* at the nation-state and sub-state level. From an operational standpoint, identity politics may lead political groups to use cyberspace operations to achieve objectives within countries or externally. Nationalist identities can be used as a communications tool for organizing, or as a weapon of conflict to use against the state or on behalf of it. Within China, nationalist narratives in the Chinese Communist Party, the People's Liberation Army, and political movements in Taiwan, Hong Kong, Tibet, and the mainland have impacted China's domestic and foreign policy since the founding of the

People's Republic of China.[56] In India, extremist right-wing forces have used electronic platforms to disparage minority communities, at times exacerbating tensions and enabling communal violence.[57] **Escalation in the Pacific** and **The Beijing Cyberconsensus** both deal with these issues.

- *The internet plays a powerful role in fostering and hardening political narratives.* While the internet brings people together and allows for exposure to new ideas, it also creates pockets of *communications systems* whereby citizens increasingly lack exposure to ideas and stories outside their group identities.[58] In the worst-case scenario, online communications enclaves can harden extreme views within a portion of the population that can then exert significant influence and seek political objectives that are opposed to the well-being of the population as a whole, potentially placing social stability at risk.[59] As technologies mix with nationalist sentiments in India and China and countries across the region, this mixture of nationalism and the internet can lead to tensions between and among states or sectors of society as hardline voices articulate their views and lead to political action within a polity or internationally. In a complex and interconnected world of cybervulnerabilities and online media, the future of security may have as much to do with how we imagine and speak about each other online as with how we protect ourselves against criminals or foreign powers that may seek to push a state off balance in the physical world. **Escalation in the Pacific** explores issues of nationalism and activism explicitly.

- *Asian cultural influence on a once largely "Western" technology.* The internet was born and incubated over thirty years in the West.[60] From the Internet Assigned Numbers Authority (IANA)[61] to root servers—and through the emergence of global technology giants like Amazon, Apple, Akamai, Google, and Microsoft—the organizational and physical structures of the internet emerged in the United States. Over the next decade, Asian perceptions of trust, security, and data may play a more prominent role in the development and shaping of the internet, on the basis of the number of online users from Asian countries alone. China and India's views on internet governance, for instance, may figure more prominently—as **The Beijing Cyberconsensus** examines.

KEY QUESTIONS

Each scenario in this report raises questions about the future. In **Hack the Farm**, multinational corporations introduce a new technology with its own security vulnerabilities into the Indian agricultural sector. A cyberincident then draws out tensions between established power holders—the regional capitals and Delhi—and the periphery of organized farming organizations. In **Escalation in the Pacific**, tensions between the United States, Vietnam, and

China raise questions about norms and potential rules for governing cyberspace operations between great and rising powers. Finally, the **Beijing Cyberconsensus** explores China's role in influencing a regional multilateral organization to achieve its political and strategic objectives, and considers how other states may respond to China's actions.

Each scenario raises questions for policymakers responsible for economic development and foreign policy, for planners responsible for developing diplomatic and military options to deter and respond to cyberattacks, and for companies that may seek to enter new markets and plan new investments. Questions include:

1. How can populations learn to adapt and address security vulnerabilities within technologies that are constructed overseas?

2. What can companies, state governments, and national governments do to help populations manage rapid technological change?

3. In the event of a cyberincident, what political and policy opportunities might emerge from a moment of political and military conflict?

4. How might governments and companies prepare to manage the impacts of longer-term issues like technology's slow influence on Asian politics and society, or changes in internet governance that may be required in Asia?

Readers can keep these and other questions in mind as they explore the scenario narratives.

SCENARIO 1

Hack the Farm

INTRODUCTION

This scenario imagines a future where multinational suppliers sell advanced agribusiness technologies into the Indian agricultural sector without providing effective cybersecurity tools, and Indian farmers and state governments lack effective capacity to mitigate the risks that they face. A cyberincident ensues and forces farmers, the Indian government, and multinational suppliers to cooperate in new and unaccustomed ways.

By one estimate, the global demand for agricultural equipment will rise by 7% annually, reaching $216 billion in the next two years.[62] The bulk of this equipment will feature digital technologies.[63] The Asia-Pacific region is poised to receive 46% of that agricultural equipment, with China contributing over one-third of global sales.[64] The digitization of the agricultural supply chain will be pervasive, ranging from tractors and machines that facilitate rowing and seed planting, crop dusting, and irrigation, to end-user technologies for monitoring livestock and assessing weather patterns. Many industry giants have already categorized their products as “smart” or “efficient” agricultural systems that run on predictive software.[65] Klaus Josef Lutz, the Chief Executive Officer of BayWa, the German manufacturer of agricultural equipment, has said that “[c]urrently [smart devices are sold to] small plantlets with sales in the single-digit millions. But long term, it will be a mainstay in our product portfolio.”[66] John Deere, which controls 60% of the agricultural equipment market in the United States, first pioneered autonomous tractors in 2002 and has sold "at least 200,000 Deere machines that can wirelessly transmit agronomic data to remote servers" located anywhere in the world.[67]

The digitization of agricultural equipment and the introduction of smart systems that rely on predictive analysis have consequences for Asian economies. Modes of Asian occupation are shifting dramatically. The 2011 Census of India, for instance, estimated that the number of cultivators in the country dropped from 50 percent in 1951 to 24 percent of the population in 2011.[68] Given the decreasing percentage of farmers as a part of the total workforce and increased demand for food, Asian farming communities, like their counterparts in America and Europe, will rely on advanced agricultural technologies to save costs and resources.

Table 1: Major Global Agricultural Equipment Suppliers

Company	Location	Components Supplied	Additional Information
Deere & Company	Headquarters: USA Plants: Mexico, Brazil, China, Canada, India, Spain	Full-line manufacturer	Biggest manufacturer in the world
Mahindra & Mahindra	Headquarters: India Plants (in India): Zaheerabad, Mumbai, Nagpur, Rudrapur, Jaipur, Rajkot, Mohali	Full-line manufacturer; low-cost supplier to Asian markets	
Tong Yang Moolsan	Headquarters: South Korea Plants: South Korea	Tractors but also power tillers, mowers, combine harvesters	
Kubota	Headquarters: Japan Plants: Japan, Thailand, Indonesia, China, Australia, Malaysia, Brazil, USA	Full-line manufacturer	
SAME Deutz-fahr	Headquarters: Germany Plants: China, India, Croatia, France, Turkey	Tractors	
CNH Global	Headquarters: The Netherlands Plants: USA, Italy, France, Brazil, China, UK, Canada, Belgium, India, Australia, Spain, Czech Republic, Turkey, Russia, South Africa	Full-line manufacturer	Second biggest manufacturer in the world
AGCO Corporation (Allis-Gleaner Corporation)	Headquarters: USA Plants: USA, Germany, France, Italy, China, Finland, Malaysia, Brazil, Canada	Full-line manufacturer	
CLAAS	Headquarters: Germany Plants: France, Russia, Hungary, USA, India	Tractors, forage harvesters, combine harvesters	
Yamabiko Corporation	Headquarters: Japan Plants: Japan, Belgium	Sprayers, crop dusters, harvesters	

* Statista, "The World's Largest Farm Machinery Manufacturers in 2015, Based on Revenue (in Million U.S. dollars)," accessed April 20, 2017, https://www.statista.com/statistics/461428/revenue-of-major-farm-machinery-manufacturers-worldwide/.

Many agribusiness suppliers are based in the United States or Europe. Table 1 lists the world's major manufacturers of agricultural machinery, their place of incorporation, and the locations of their plants. This table is revealing: some corporations, mainly those based in Japan and South Korea, have plants or manufacturing facilities in the Asia-Pacific, but the digital supply chain over the next decade will largely comprise products imported from North America or Europe. As supply chains for agricultural technologies become more diverse and geographically separated, Asian agrarian economies will likely have fewer means to manage, identify, and mitigate security vulnerabilities. This scenario reflects one such instance; the Yamaha R-Max 2 drone is left vulnerable through its default security settings.

KEY DRIVERS

Four key drivers and elements may come together to create an "agricultural equipment hack": the increasing appetite for digitized agricultural equipment in Asia; inadequate cybersecurity awareness of farmers (especially first-generation internet users) and state governments; the growing frequency and sophistication of cyberattacks; and the lack of robust information-sharing channels among law enforcement agencies.

First, a rise in demand for resource-efficient agricultural technologies may lead to the increased inflow of foreign products into the Asia-Pacific. Farmers in the region who use digitized agricultural equipment are likely to be first-generation internet users.[69] Without the required skills or training in cybersecurity, they will be vulnerable to attacks, particularly if they lack connections to an effective institutional support network.

Second, corporations have made their IoT systems user friendly for operations (if not for technical maintenance),[70] making them an attractive option for farmers or other cultivators who are unfamiliar with digital components in machinery. Uninformed users may lack effective control over smart machines, making those machines into a lucrative target for illicit attacks as criminals steal data for their own advantage.[71]

Uninformed users may lack effective control over smart machines, making those machines into a lucrative target for illicit attacks as criminals steal data for their own advantage.

Third, criminal actors could use ransomware to make farmers pay for the continued use of smart devices. At a strategic level, nation-states could use malware as a tool of economic warfare to damage another nation's agrarian economy. Many such attacks could go undetected or unreported in cases where the end users fail to gauge whether a device has malfunctioned because of a technical glitch or an act of mischief.[72]

Finally, a lack of effective law enforcement channels to share information about cyberattacks compounds these problems, especially in emerging economies. Since suppliers of digitized agricultural equipment are often based in jurisdictions outside of their home countries (with few domestic manufacturing plants in Asia, as Table 1 illustrates), law enforcement agencies have limited options to investigate and prosecute criminal activities. In countries like India that lack an effective IoT security policy[73] and where product testing is mostly confined to mass communications devices like telecommunications infrastructure and mobile devices,[74] in the event that a vulnerability is discovered in a foreign good, Indian regulators may simply impose higher fines to penalize suppliers of agricultural equipment. This has already happened in the case of telecom or ICT equipment, with mobile operators bearing the brunt of security regulation of hardware.[75] The scenario explores these and other drivers as they may unfold following a cyberattack.

SCENARIO

It is 2020 and several state governments in India have successfully entered into contracts with Japan's Yamaha Motors[76] to provide affordable Unmanned Aerial Vehicles (UAV) that can be used as crop-dusters. The Yamaha R-Max 2,[77] a highly sophisticated and autonomous UAV with built-in GPS, is an improvement from its predecessor. Farmers no longer need to control the drone through radio, and the intelligent machine can learn, quantify, and drop the exact load of required chemicals over the fields.[78] For India's aging agrarian communities, where second- and third-generation family members are increasingly reluctant to take up farming, the UAV promises to save time, money, and energy.

Yamaha, which operates its UAV in South Korea, Australia, and the United States, is the latest entrant into the digitized Indian agricultural market.[79] The U.S. Federal Aviation Authority (FAA) approved the R-Max's license in 2015,[80] and the UAV achieved tremendous success in places like Napa Valley, where helicopter units charge hefty rates for spraying vineyards.[81] In India, Yamaha eyed the cotton belt states that straddle the country: Gujarat, Maharashtra, Telangana, Andhra Pradesh, Madhya Pradesh, and Rajasthan.[82] Cotton is a water-intensive crop that consumes nearly 60% of all pesticides used in India annually.[83] While central India's cotton plantations may not be the sprawling fields of Napa Valley, crop-dusters can help by periodically spraying pesticides and water over larger tracts of land.

Soon after the R-Max 2 is licensed to enter the Indian agricultural market, Indian farmers deploy it with moderate success. The cotton belt states utilize it widely, easing the resource-intensive job of crop-dusting with technology.

Many farmers use UAVs for the first time and require digital training to operate the devices. Buyers allow the UAVs' systems to automatically patch and update their software. Ahead of the dusting season, the R-Max 2 receives a firmware upgrade that will purportedly improve its GPS system. In reality, the patch is malicious code injected to tamper with the UAV's load monitoring tools, resulting in the spraying of pesticides and water in excess over agricultural fields. Although warning signs against unreliable or malicious updates to Internet of Things (IoT) firmware have been in existence for some time,[84] this virus finds its way to the crop-dusters.

The "patched" drones ultimately destroy crops across the cotton belt, with the cybersecurity problem going undetected for at least a week. The farmers, represented by trade unions and lobby groups, blame Yamaha and demand accountability from their state governments. Since the agrarian community is an effectively mobilized and vocal constituency, the cyberattack on the R-Max 2 drones sets off a political and economic crisis. The state governments lack the capacity or tools to identify the source of the hack and approach the Prime Minister's Office for help.

> The "patched" drones ultimately destroy crops across the cotton belt, with the cybersecurity problem going undetected for at least a week.

The Prime Minister's Office directs the National Cyber Security Coordinator (NCSC) to run a three-member commission to investigate the attacks and submit a fact-finding report in three weeks. The NCSC-led committee's report is scathing: it identifies the cotton belt states as having done little to prepare or build capacity in farmers who were using sophisticated, digitized agricultural equipment for the first time. The attacks seem to have originated from numerous jurisdictions, some of which have no mutual legal assistance treaty (MLAT) or information-sharing channels with India. The perpetrators remain at large and unidentified. The Bharatiya Kisan Sangh (BKS), a farmers' union with powerful political affiliations, conducts a nationwide agitation to protest the use of autonomous crop-dusters in India. Under enormous pressure to take responsive measures against the hack, the government of India suspends the use of all new Yamaha agricultural machines pending a comprehensive review of their security concerns.

POTENTIAL OUTCOMES

While the drivers behind a major cyberattack on agricultural machinery in the Asia-Pacific may be economic or technical (i.e., poor security), such an attack would trigger political changes by the Indian government and the farming community. Given that most growing economies in the Asia-Pacific continue to be predominantly agrarian, cyberattacks on agricultural machinery would receive political visibility, eliciting a strong reaction from state governments. Moreover, repeated cyberattacks on digitized farming equipment may lead agrarian constituencies in India and other major Asian markets to lose confidence in these machines. Potential outcomes include the following:

Demands for accountability. Governments in the Asia-Pacific would engage each other in a game of finger-pointing in the aftermath of a cyberattack on agricultural machinery, especially given the regional governments' difficulties in attributing or identifying sources. Such attacks would raise domestic and international political tensions since agrarian communities, especially in South and Southeast Asia, are an influential constituency capable of mobilizing political attention from their respective governments. If the attack is widespread and affects crop output, governments would be pressured to identify response options to retaliate against other states or non-state groups.

Stronger supply chain controls. Governments are already concerned with globally distributed digital vulnerabilities and poorly monitored ICT supply chains. The UN Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security suggested in 2015 that states take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.

Although a vexing problem to solve given issues of global jurisdiction, a major, disruptive attack on agricultural machinery would prompt governments to focus with renewed energy on digital supply chains. Specific actions might include imposing extra-territorial liabilities on corporations, or potentially creating licensing regimes to ensure that companies comply with nationally determined security standards. If ill-considered, regulation could place a heavy burden on foreign manufacturers as they try to enter global markets.

Past discussions of supply chain integrity have focused largely on ICT products, and American entities like Microsoft[85] and the U.S. government have played prominent roles in the conversation.[86] In this scenario, internet companies would need to work closely with agriculture equipment giants like General Motors, Monsanto, and British Petroleum to address their industrial IoT risks. If malicious actors increasingly target the ICT components of agricultural machinery or industrial equipment, manufacturers will likely face higher costs in areas such as cybersecurity and liability insurance for their automated and digital technologies. Such events would likely lead to regulatory conversations as well as innovative research and development partnerships and potential joint ventures to advance IoT security.

Reduced agricultural productivity. While agricultural output accounts for less than 4% of the world's GDP today,[87] several Asian countries continue to be primarily agrarian. Agriculture makes up nearly 17% of India's GDP and 27% of Pakistan's GDP, for example.[88] In Southeast Asia, Singapore has weaned itself from agrarian output as a factor of its economic development. In nearby Cambodia, farming constitutes 30% of the national GDP.[89] Large-scale or even isolated but dramatic cyberattacks on digitized agricultural equipment could discourage farmers in Asian countries from relying on frontier technologies and lead them instead to continue their use of traditional methods of cultivation, potentially affecting growth and competitiveness over time.

Cybersecurity cultural change. Following a scenario like this one, multinational corporations would be likely to amend their cybersecurity capabilities to become more user friendly and to make their devices more secure. As corporations amend their cybersecurity practices, the Indian government would likewise consider initiating a popular campaign of basic cybersecurity best practices and use the incident as a rallying point for improving the country's approach to cybersecurity across sectors.

Multinational corporations would likely amend their cybersecurity capabilities to become more user friendly and to make their devices more secure.

If developing countries have struggled to build awareness about the need for cybersecurity to date, as internet access grows, populations may come to see the internet as indispensable to their livelihoods over time. This would lead to a slow, evolving cultural change in how Indians treat technology, seeing it perhaps as a tool that requires care and attention. Such a slow cultural change over time could lead to an improvement in India's cybersecurity response capabilities at the governmental and individual levels.

CONCLUDING LESSONS FOR POLICY PLANNERS AND STAKEHOLDERS

This scenario raises a number of policy and regulatory questions for investors and policymakers to consider as advanced technologies enter into the Indian market. These key questions focus principally on cross-sector planning opportunities, regulatory environments, and risk management options for communities unaccustomed to advanced technology and cybersecurity.

A major cyberattack on machine-driven economic systems would carry geopolitical consequences and policy implications that extend beyond the sector in question. Advances in machine learning today herald a new phase in the information revolution, a phase marked by the automation of jobs and services.[90] Policymakers and investors concerned about the future of security and economic productivity should consider the potential cybersecurity consequences of large-scale automation across sectors, from automated cars to industrial equipment to personal devices in the home that control thermostats or food production. Each sector will need to imagine the future and explore implications of automation, looking specifically at cultural and political issues in Asia. A range of lessons and questions follow.

A major cyberattack on machine-driven economic systems would carry geopolitical consequences and policy implications that extend beyond the sector in question.

The role of multinational corporations. An event like that described in this scenario could also draw the attention of industrial giants in traditional sectors—such as U.S. Steel, China National Offshore Oil Corporation (CNOOC), and Exxon—that may have previously played a marginal role in the evolution of cybersecurity practices. Some corporations like Ford have already invested in cybersecurity analysis in light of the projected future of self-driving cars,[91] while other industrial giants may not have invested in automated products to the same degree. Such large companies all have significant resources to lobby and influence policymaking, and their early involvement and adoption in IoT security planning could help mitigate long-term risk. What partnerships and initiatives can companies and governments form now to address the potential risks posed by increasingly autonomous systems, particularly in sectors that to date have been largely unaccustomed to advanced technologies, like the agrarian industry?

Getting the basics right and capacity building. Although this scenario outlines a cyberattack on a traditional sector, the parameters used to assess the attack are the same as on any digital network or infrastructure: prevention, detection, and response. In this case, a firmware update introduced malicious code into the crop-dusting drones, but the response process is as much a question of cyberhygiene and user action as it is about the manufacturer's liability. Where will insurance underwriters place the onus of responsibility in the event of an incident, and what protections will farmers or other users receive against corporations that could be liable for an incident? How can the legal and court systems prepare for the impact of autonomy on society? Do farmers bear a responsibility to check patches before installing them, or is Yamaha (in this case) wholly liable for any damage caused?

It is likely that the law, especially in emerging economies, will place a heavy burden on the manufacturer as it does with service providers. By analogous example, the Reserve Bank of India's draft circular on "unauthorized electronic banking transactions" suggests that the customer will have "zero" or "limited" liability in almost all cases of breach.[92] Where there is a "third party breach, where the fault lies neither with the bank nor with the customer but lies elsewhere in the system," the customer needs only to notify the bank quickly to absolve herself of liability. The draft circular states that the onus is on the bank to address fraud complaints within 90 days. Yet the circular does not mention how legal liability is addressed when fraud or theft is caused as a result of a cyberattack or a vulnerability exploit.[93] A cyberattack on Yamaha's crop duster may thus lead to a bevy of litigation against the company, but the legal regime of rights and responsibilities needs to be clarified.

In matters of organizational response, how would farmers and others engage the Indian government as the scenario unfolds? Given the relatively low public awareness of the Indian Computer Emergency Response Team (CERT-In), for this kind of event, it is unlikely that farmers or their collective would report the incident, but rather would treat it as a technical complaint to be addressed by the company's representatives in India. Companies or services that provide technology-enabled equipment are not likely to instruct their customers in developing countries on the basics of cyberhygiene, which in this case would mean holding off on installing automatic firmware updates until confirming their veracity and benefit. There is a clear role for government to play in promoting awareness about cybersecurity and to try to protect citizens against disruptions. It is therefore incumbent on policy planners to address capacity building issues that will arise as a result of the digitization of the agricultural sector.

How would farmers and others engage the Indian government as the scenario unfolds?

Develop legislation to secure the IoT ecosystem. A cyberattack on Internet of Things-based applications may spur domestic and international interest in regulating IoT infrastructure. A catastrophic attack would lead to the creation of legal regimes that shift liability onto IoT suppliers, especially given that emerging economies often lack the resources to protect their own digital assets. At the same time, restrictive legal regimes may discourage investment and innovation in the IoT ecosystem. As stakeholders plan for IoT security, they should place regulation at the top of their planning agendas as IoT extends from the home to industrial use at a larger social scale.

Conduct comprehensive planning for cybersecurity risk management. Cybersecurity risk is a factor not only of the security of digital networks, but also of the capacity of individuals and companies to adapt to changing security and technical norms. Coming out of this scenario, the message to government officials responsible for industrial and agrarian risk management is clear: cybersecurity is no longer the province of the IT sector alone, as digitization extends across economic sectors.

Cybersecurity managers may not be able to anticipate every risk, but they can identify the dynamics that could emerge when advanced technologies become a part of a particular sector's work practices. Were Yamaha or John Deere or another multinational company to introduce new IoT equipment into India, policymakers could imagine the potential risks and begin to engage constituencies in a multi-stakeholder risk management process that draws in insurers, public educators, and corporate engineers.

There are a number of steps that corporations and political leaders can take to get ahead of risk. Practically, multinational agricultural equipment companies and other IoT producers should consider the *simplest set of cybersecurity instructions for end-users* who may or may not be accustomed to risk management or prepared for disruptions. Politically, corporations should consider *how and when the introduction of new technologies may exacerbate pre-existing political tensions,* like feelings of disenfranchisement between farming communities and the government. It is not a company's responsibility to help the government, but it is a company's job to consider social impacts before it introduces a new technology, and to identity potential areas of friction and try to help mitigate those risks before introducing a tool into a country. Governments may consider *investing political capital and time in strengthening relationships* between end-user communities (in this case, farmers), and state and national government offices responsible for managing constituent issues.

Corporations and governments can achieve long-term benefits by making *a relatively small analytical and organizational investment in industrial IoT risk management.* Possible opportunities for investment could include:

1. Public-private information sharing and collaborative forums between security agencies and corporations investing in internet-enabled technologies;

2. Designated cybersecurity-oriented staff within government agencies that can conduct outreach to at-risk sectors, such as the agricultural sector, or to supervisory control-data

acquisition (SCADA) managers in critical infrastructure companies that may have limited experience with cybersecurity.[94] Simple briefings to unions, meetings with mayors, and local corporations and newspapers can all help.

3. Designated staff within corporations tasked with considering potential downstream risks that may emerge when consumers encounter internet-enabled technologies on a scale such as that outlined in this scenario. A single well-informed, capable, and communicative staffer can make a significant difference in building partnerships and capacity.

History shows that organizational structures need not be large to be successful. In this case, cybersecurity teams can be staffed initially with one or two people close to the executive suite who can coordinate working groups across sectors, direct research and communications to inform managers about risk, and conduct outreach to relevant constituencies.[95]

Hack the Farm

KEY TAKEAWAYS

The expanding use of advanced agricultural drone technologies across India's cotton belt leaves the farming economy vulnerable to cyberattacks. **Key drivers in the unfolding of the scenario include** cybersecurity vulnerabilities in India's developing economy, and Indian society's relative unfamiliarity with cybersecurity risks; the Indian government's lack of institutional controls and expertise for dealing with cybersecurity, particularly in rural areas and agricultural communities that are unfamiliar with advanced technology; and evolving legal and insurance regimes for risk. Political tensions between the "haves" in New Delhi and regional capitals and the "have nots" in farming communities—and the political narratives and differences between them—would come to the fore in the event of a disruptive attack. A disruption would drive diverse communities together as farmers, policy planners, and multinational companies would work to remediate an attack and prevent future incidents.

Cybersecurity policy and strategy choices. Companies can work to undercut the cybersecurity risks they face when entering diverse markets that may be unfamiliar with technology. This scenario highlights clear benefits of advanced planning across sectors to educate diverse communities and develop small-scale solutions that carry large payoffs. On the government side, India can begin planning now to step up its national cyberhygiene communications and develop a regulatory framework for preventing disruptions caused by foreign-built technologies. Companies, governments, and communities can work together to build more secure systems and foster resilience by increasing information sharing, creating public-private forums, and investing in small cybersecurity teams to mitigate technological and political risks that may arise as India and other countries expand their internet access significantly.

SCENARIO 2

Escalation in the Pacific

INTRODUCTION

This scenario deals with a significant known concern for international security and cybersecurity in Asia: the potential for escalation between the great powers of China and the United States following a destructive cyberattack. As this study has shown, Asia is a region of rising economic powers; it contains within it a range of unresolved border disputes and lacks a robust regional security architecture, like NATO, to help deter and resolve disputes between greater and lesser powers. The region is a tinderbox with a range of potential triggers. Cyberspace operations now provide an added layer of complexity, driving security planners in the United States, China, and around the world to consider how actors might interact in a crisis. Any study of Asia's cybersecurity future must consider an escalation scenario involving the world's two great Pacific powers.

Any study of Asia's cybersecurity future must consider an escalation scenario involving the world's two great Pacific powers.

In this scenario, the root cause of the escalation resides in a territorial dispute in the South China Sea between China and Vietnam, a U.S. ally that has frequently been the victim of Chinese bullying and has often found itself alone in confronting China's assertiveness in the region. China and Vietnam contest maritime borders in the South China Sea (and elsewhere) to such a degree that anti-Beijing riots broke out in Vietnam after Beijing moved an oil rig into Vietnamese-claimed waters in 2014.[96] The nature of China's political behavior with Vietnam and across the region is central to the scenario—and forces within and outside of China would shape China's actions as it interacts with its neighbors and others.

In the event of escalating tensions with a neighbor, how would China respond to a foreign cyberattack on its networks and systems? Has China prepared potential response options and considered proportionality for such a contingency? A cyber-enabled dispute involving China and other nations addresses all three premises at the core of this study: vulnerabilities in Asian networks, the rise of China's economic and military power and its impact on the region, and unresolved differences of opinion regarding proportionality and the Law of Armed Conflict in governing cyberspace operations. In this scenario, international forces exert themselves amidst a backdrop of domestic political and technological change and transition within China itself.

KEY DRIVERS

This scenario also explores a range of political drivers. These include divergent perceptions and expressions of Chinese nationalism within the Chinese Communist Party, the People's Liberation Army, the Chinese population, and Vietnamese political groups. The study also looks at class tensions between the Chinese middle class and the governing elite, as well as the dynamism inherent in the United States-China relationship. China's disregard for international arbitration regarding the South China Sea provides a further trigger for the scenario.

In addition, two scenario-specific key drivers impact political and governmental behavior as the story unfolds. First, government and private investments in technology have led to a more wired Chinese population. Industries from manufacturing to entertainment to journalism rely more on data for operations than in the past.[97] At the same time, the CCP's "Great Firewall" web monitoring and blocking capability curtails freedom of expression and connection with the outside world, and the CCP spends billions of dollars in domestic online surveillance.[98] Despite the government's efforts toward consultative engagement with the Chinese people,[99] the CCP continues to suppress political dissent and organization in the physical world as well as in cyberspace.[100]

Second, externally, over the last decade the People's Liberation Army (PLA) and the Ministry of State Security (MSS) have conducted global cyberespionage operations, as well as gradually developed their cyberspace operations capabilities and incorporated them into doctrine. Planned operations by the PLA could include targeting the military planning, communications, and logistics capabilities of the United States or its allies to disrupt data and affect operations.[101] Increased cyberspace investments would leave the United States and other Asian nations concerned about how China may act, particularly given China's refusal to adhere to the Law of Armed Conflict. All of this provides a backdrop to the scenario's events.

SCENARIO

In mid-2020, following a few years of economic decline,[102] China's economy takes a plunge. The middle class shrinks for the first time in decades. Whereas at one time broad societal concerns regarding environmental pollution and the Great Firewall could be partially subsumed through China's continued economic growth, in mid-2020, long-dormant political frustrations begin to fester in the population.[103] The impacts of the slowdown are significant, particularly at the nexus of technology, domestic politics, and foreign policy.

First, the slowdown leads to a moderate increase in political dissidence within China. Sectors of the elite across society grow disenchanted and place pressure on the Chinese Communist Party (CCP) to reform its economic policies. The middle class grows increasingly vocal and begins to organize protests online and in the real world.

As a result, China takes seemingly desperate action abroad. In the face of a depreciating yuan, China shores up its energy resources in the South China Sea, in contravention of a declaration by the Permanent Court of Arbitration at The Hague regarding China's claims to the region.[104] China moves its $one-billion Haiyang Shiyou 981 oil rig[105] back into waters near the Paracel Islands to pump oil from a part of the South China Sea that is controlled by China but claimed by Vietnam. This action follows the previous dispute between the two countries in 2014 and 2016 over the presence of the rig in waters claimed by Vietnam.[106] In that case, the Vietnamese government protested the move formally through *démarches* and raised the issue within ASEAN.

This time, the Vietnamese take action in response. Vietnamese nationalist hackers unaffiliated with the government break into the networks of the China National Offshore Oil Corporation (CNOOC) and manipulate data acquired and stored through the Haiyang Shiyou rig's operations. The plan for the hacktivist attack on CNOOC had been developed over years in response to a prior incident—when a Chinese national hacked into Vietnamese airport monitors in July 2016—but only made sense to execute after the Chinese rig entered Vietnamese waters.[107] CNOOC recovers quickly from the cyberattack, largely due to investments in back-up capabilities that allow business operations to continue unabated.

The Chinese Ministry of Foreign Affairs attributes the hack to Vietnamese citizens and calls it a "juvenile attempt to disrupt China's legitimate effort to pursue its national economic interests." The Vietnamese government claims that the hack "brought shame onto Vietnam" and vows to control the hacktivists; the CCP leadership believes that the hacktivists acted in cahoots with the Vietnamese government.

The conflict escalates. The PLA covertly penetrates the networks of Cho Ray Hospital in Ho Chi Minh City for purposes of surveillance and collection on key leaders. During the surveillance operation, a young PLA major inadvertently tests malware that destroys data regarding the timing and delivery of medicine to two wards of patients. In the first known deaths caused by a data-disruptive cyberattack, four patients die at Cho Ray hospital from failing to receive adequate amounts of medication through their medical devices. Among the victims are two Americans, one of whom happens to be the diabetic cousin to the U.S. Charge D'Affaires in Hanoi.

In an interview on BBC Asia, a spokesperson from a private American firm contracted by the Vietnamese government attributes the hospital attacks to the People's Liberation Army. The Chinese Ministry of Foreign Affairs denies the attack.

The United States' response. The U.S. government sends a delegation of cybersecurity experts to Vietnam to assist in forensics investigations and help secure the country's infrastructure. The U.S. intelligence community fails to identify a clear motive, but given the lives lost, the U.S. National Security Council directs the Treasury Department to explore potential sanctions against the Chinese government.[108]

In conversations with the U.S. President, President Xi denies China's involvement in the attack. In a major shift in Chinese policy, however, he offers that rules for cyber operations must follow the Law of Armed Conflict, anticipating the U.S. President's diplomatic position regarding the norms of operations in cyberspace. The U.S. President explains that, given clear violations of sovereignty and the death of American and Vietnamese citizens, the attack was unwarranted and dangerous and that China overreacted. President Xi expresses regret for the loss of the Americans' lives and affirms his desire to continue productive relations with the United States across a range of issues. At home, President Xi's team initiates a full investigation into the conduct of the PLA's cyberspace operations team. The military conducts a trial and finds the PLA major guilty of involuntary manslaughter.

President Xi denies China's involvement in the attack.

The U.S. Secretary of State asserts in a public statement that "destructive cyberattacks cannot be tolerated within the international system. States must recognize norms in the conduct of such operations, just as they would in the physical world. The United States and China have made progress on cyber norms in the past and should do so again." His position provides a counterpoint to the actions of the Department of Justice; the next week, in a case prepared over a period of years, the U.S. Attorney's Office in Missouri indicts two brigadier generals, three colonels, and five majors within the PLA and holds them responsible for international intellectual property theft against a financial management firm in Kansas City.[109]

Domestic activism in China. Back in China, economic frustration leads to increased political activism, further calls for economic reform, pressure on the CCP to remove internet constraints, and an expansion of the rule of law to protect freedom of expression.[110] Such activism emerges out of a growing belief shared by many in the middle class that the CCP has failed to meet their economic aspirations. Reports of China's cyberspace activities in Vietnam are a secondary driver of popular protests; intellectual dissidents argue that the PLA acted rashly in the cyberspace operation and placed China's interests and values at risk, and they argue that the sanctions are a direct result of mistakes by a government that is now responsible for economic malaise and foreign policy mismanagement.

The Chinese government responds by jailing dissidents, tightening the Great Firewall around social media platforms, and threatening to shut off chat capabilities and mobile online payment tools for citizens who participate in public demonstrations. Within a week, usage rates of encrypted circumvention tool tools rise from hundreds of thousands to millions.[111] A group of young PLA soldiers declare themselves "loyal soldiers of the people" and organize an internal cyberspace operation against the state. Using infrastructure in Vietnam, Thailand, and the United States, the former PLA hackers shut off governmental

surveillance capabilities in Beijing, Shanghai, Guangzhou, and Hong Kong for a period of hours. The CCP's response is swift. All five members of the dissident group are detained and their families' homes raided.

Within the military leadership, two camps emerge. The first is composed of those who would seek stability to preserve the CCP's control over the country. A second group seeks a modicum of reform to allow for greater freedom of expression and to sustain economic growth at all costs. The two take divergent actions and lobby President Xi and the Central Military Commission (CMC) accordingly.[112]

POTENTIAL OUTCOMES

This scenario, in which an external cyberspace operation inadvertently triggers domestic unrest, would raise a number of medium- to long-term issues in cyberspace operations and cybersecurity policy, and could lead to a range of outcomes within China and for the international system broadly.

Domestic Outcomes In China

This event places Chinese President Xi Jinping in a position of constrained decision-making. He would feel pressure to manage the nation's economic development and social stability and maintain a productive relationship with the United States and Vietnam during an emerging crisis. At the same time, he would seek to maintain his legitimacy with an element of the military over which he had previously sought to exert greater control. President Xi would feel compelled to accommodate the vocally nationalist elements from across sectors of society, from the PLA to elite corporations to average citizens who seek a muscular response to Vietnam's actions. As he balances these internal political realities, President Xi would be keenly aware that his actions on domestic internet control policy and foreign cyberspace policy have the potential to impact his country's economic and security future for years to come.

This event places Chinese President Xi Jinping in a position of constrained decision-making.

Depending on Xi's decisions, three potential outcomes of domestic unrest would include: (1) deepening CCP resilience and control over the PLA and body politic; (2) a loosening of restrictions on freedom of expression; and (3) unrest within the country and dissent within the PLA.

Outcome 1: CCP crackdown and consolidation. The CCP could sustain itself by allowing only the barest of accommodations to activists while punishing members of the PLA and attempting to solidify President Xi's control over the military. Economic reforms from the top, required to manage the economic crisis, would not necessarily include an expansion of democratic and political rights. Indicators of this outcome would include a further expansion of social controls, increased jailing of dissident groups, and expanded ideological control over the PLA and other aspects of the Chinese bureaucracy. In other words, there would be a ratcheting up of government suppression.

The PLA's internal dissent would likely be of greatest concern to the CCP and could lead to a significant expansion of the role of the People's Armed Police (or other security forces) in monitoring dissent.[113] Crackdowns within the PLA and People's Armed Police would compound preexisting mistrust following President Xi's military reforms of 2015.[114] The CCP would need to prevent future dissent without alienating an important constituency.

In matters of foreign policy, this outcome would likely force President Xi and others in China to focus on domestic activities at the expense of external strategy, thus leading to a potential decrease in China's geopolitical influence in the short term—especially as China would be focused on trying to resolve disputes with Vietnam and the United States at the same time. Consolidation and suppression would be a concern to anyone watching Chinese markets.

Outcome 2: Moderate increases in freedom of expression. A second potential outcome within the CCP could be a combination of measured opportunities for increased freedom of expression combined with elements of consolidated control over specific elements of Chinese society, including the PLA.[115] President Xi and the CCP would have anticipated the economic unrest following the Arab Spring and put plans in place to allow for increased dissent, the "next phase" of the pro-forma 2011 expansion of consultative democracy. The Great Firewall would open further, and the population would be given access to some foreign news sites. Cyberspace would become a domain of greater political activism and communication.

President Xi and the CCP would have anticipated the economic unrest following the Arab Spring and put plans in place to allow for increased dissent.

Such a path may tempt President Xi, as consolidation and crackdown could lead to a further erosion of the CCP's legitimacy within the frustrated Chinese population. Given the expanding nature of internet access, a moderate increase in freedom of expression during a period of constrained power would seem consistent with the history of democratic evolution by authoritarian states. A rapid expansion in circumvention tools and an increase in political organization would also lead to increased connections between activists and the broader political class. Over the years following these events, political activism would facilitate a broader national conversation about China's role in the world, which would be a natural evolution in China's economic and political development. This could lead to a shifting role for China within the international system that better reflects norms of responsible international behavior, including in cyberspace operations for military objectives or intellectual property theft.

Outcome 3: Chaos averted, but long-term reform becomes more likely. The level of social dissent outlined in this scenario, including cyberspace operations by elements of the population and an increase in circumvention tool usage, would be unlikely to lead to a significant political disruption or a coup against the ruling party. Earlier years of economic growth and stability, the CCP's slow expansion of freedom of expression, and China's rise within the global system are all perceived to bring power to the elite that will be loath to give up their position. As much as the middle class may feel frustration against the regime for economic policy, it would perhaps take a period of prolonged oppressive crackdown or disarray for the population to call for a major change in the political status quo.

This scenario would lead to a higher degree of coordination between activists and civil society groups and the population, however, making some element of long-term political and economic reform more likely. Activists, technologists, and journalists would develop strong ties with each other and with elements of the population through the course of this scenario, and that would help them to strengthen their position against the CCP and influence the political and economic conversation in China regarding the country's future. As China's per capita GDP increases over time, if China follows historical precedents like Hungary and Mexico,[116] activists and others will pressure the regime to democratize; the CCP may struggle to resist pressures from citizens to move toward greater freedom of expression online and more open borders in cyberspace, potentially pressuring the regime to allow foreign social media and technology firms like Facebook into China, a move that would lead to an even higher degree of coordination between groups. In the short term, however, the scenario will be unlikely to threaten regime stability given prevailing memories of China's economic growth, the elites' attachment to their position, and preferences for stability over chaos.

This scenario would lead to a higher degree of coordination between activists and civil society groups and the population.

International Outcomes

This scenario would likely change how states govern and speak about the use of cyberspace operations, especially if leaders seize the opportunity that such a high-profile incident would provide.

United States-China relations devolve and then improve. The scenario would likely pressure the United States and China (and the broader international community) to address the role of cyberspace operations in conflict escalation in a manner previously unseen, particularly given the loss of life. The response would depend largely on the degree to which media and global leaders turn the incident into a moment of opportunity for change in cyberpolicy, rather than brush the incident aside in favor of other issues associated with managing China's economic and military rise.

Positive outcomes in the medium- to long-term could include: 1) China affirming, through pressure from India and Singapore, that the Law of Armed Conflict applies in cyberspace; 2) an agreement by the United States and China on the conduct of cyberspace operations in peacetime; and (3) agreements regarding targeting limits during conflict and the preparatory stages of hostilities.

China and the United States could agree bilaterally that neither state would target a hospital or any institution of public health during peacetime or hostilities. Such an agreement would expand beyond preexisting, non-binding norms (as opposed to laws or rules) in circulation within the international community that bar certain actions in cyberspace, to include barring attacks on aspects of the internet during hostilities.[117] History indicates potential for progress in this regard. In 2015, a United Nations-convened group of governmental experts—including representatives from China and the United States—submitted a document to the United Nations General Assembly arguing that aspects of critical infrastructure that contribute to public safety should be off limits during conflict. The report states that, *inter alia*, "[a] state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[118] Although this report is not legally binding—the G7 later affirmed these principles in April of 2017 in a joint communiqué[119]—these affirmations could lay the groundwork for future agreements between the United States and China regarding potential targets that may be off limits during a conflict. An unfolding of events similar to this scenario could trigger both states to make such commitments.

Over time, the incident in this scenario could lead stronger states like Australia and Singapore to advocate within ASEAN (with the support of India) that the United States, China, India, and the ASEAN states agree not to target aspects of global critical infrastructure whose interruption could disrupt the entire global economy. Proscribed targets could include internet chokepoints that drive the global financial system, such as the SWIFT code system and the thirteen root name servers.[120] Such proscriptions would meet resistance from military strategists who seek to preserve freedom of maneuver and crisis management options for political leaders, but the instinct to take such a control action may still emerge.

Military-to-military dialogue. The incident would lead to an initial cooling off period in U.S.-China military relations, yet the loss of life would put pressure on the CCP/CMC and the PLA to reform China's cyberspace operations and policy, and China's military operations as a whole. The incident therefore would have the potential to become a moment of change for U.S.-China military relations. The PLA hacking incident could become a "catalytic event" in the evolution of China's military culture. PLA ideology and identity would change, with some officers hardening and others softening their views, impacting the U.S.-China military relationship as younger officers rise into leadership positions. Depending on how leaders manage the transition, later developments in the story could include the United States and China agreeing to an exchange of military personnel at their respective military cybercommands.[121]

ASEAN declaration of norms. A final potential outcome of this scenario would be a deepening understanding of and increased attention toward the use of cyberspace operations within the international system as a whole, beginning in Asia. At an ASEAN regional forum anywhere from six months to a year after the incident, security leaders could assert norms of operational behavior in cyberspace, decide that every state in the region should be clear about its cyberspace declaratory policy, and agree to adhere to the rule of Law of Armed Conflict in the conduct of operations. Stronger states that have often allied or sided with the United States in matters of international norms of operations—including Australia, India, and Singapore—could lead the way in the region. Such an agreement could build off or augment any statements or agreements by the United State and China in this scenario. The shift toward transparency and declaratory policy could lead to greater military-to-military cooperation across the region around cyberspace operations planning, command and control, and workforce development.

CONCLUDING LESSONS FOR POLICY PLANNERS AND STAKEHOLDERS

A scenario like Escalation in the Pacific would have repercussions for political and economic affairs in China and the Asia-Pacific, as well as for organizations concerned with cybersecurity globally. Policymakers and researchers should consider what policy, technical, and operational opportunities may derive from such a scenario.

Domestic Lessons

Nationalism, cyberactivism, and cyberoperations. In this scenario, Vietnamese nationalist hacktivists trigger a chain of events that leads to an inadvertent escalation. Following the Vietnamese attack on CNOOC, nationalist voices within the Chinese population urge President Xi to conduct reprisal actions against Vietnam, when the rational course would instead be to maintain peace and stability through diplomacy, as opposed to retaliatory measures in cyberspace that could go awry. Finally, in a period of crisis, elements of the population may seek to conduct cyberspace operations against the regime as an act of resistance when their communications or other freedoms are curtailed or suppressed. Nationalist political narratives could easily find their expression online. Cyberoperations could thus become a tool of activist attack internally—a militarist expression of underlying political views and grievances.

As nationalist expressions rise, leaders could ask themselves: beyond the use of force or social controls, what concessions can we make—or what political stories can we tell—to channel nationalist fervor toward productive outcomes for the country as a whole? What other tools could President Xi have used in this instance to alter China's future? What could he have said to undercut resistance and lead his country forward? Ultimately, political stories and concessions in a crisis will lack legitimacy without real reform, which leads to the next recommendation.

> Cyberoperations could thus become a tool of activist attack internally—a militarist expression of underlying political views and grievances.

Absent a just rule of law and a legitimate government, activists in authoritarian or illiberal regimes in Asia will likely turn to cyberspace operations as a form of resistance during periods of crisis or tension.[122] In 2016, Freedom House ranked the majority of Asian countries as of 2016 as either "not free" or "partly free" when it comes to freedom of the internet;[123] citizens are limited online and offline in what they can say and do politically. While some citizens may accept social controls during periods of political stability, a socio-political crisis like that outlined in this scenario can spur online and offline activism, as was seen *inter alia* during the 2011 Arab Spring[124] and the 2014 Hong Kong pro-democracy protests.[125] In the face of systemic oppression and illegitimacy, political actors in Hong Kong, Tibet, Taiwan, and other restive regions across China may choose to conduct cyberspace operations out of resistance to the regime's online social control mechanisms. The hacker conglomerate Anonymous reportedly conducted cyberattacks against China as a form of political resistance during pro-democracy protests in Hong Kong in 2014, defacing webpages.[126] The destructive and disruptive capabilities of such groups will likely increase over time.

In such cases, a security situation cannot be materially improved through "better cybersecurity," as hackers will simply try different modes of attack, but rather by improving political and economic realities for the population. In China's case, this would include furthering a just rule of law that protects all citizens and developing a system of government that allows for a measure of self-determination, autonomy, or political representation, as well as dissent.[127] Absent these ingredients, during future tensions activists can be expected to take their grievances online in the form of cyberspace operations.[128]

International Lessons

Some targets off limits. Certain civilian systems of public health and safety remain vulnerable to disruption and data vulnerability, placing civilians at risk. In matters of diplomacy and interstate conflict, states may be able to improve international security by considering which systems should be considered off limits, including systems of public safety or those responsible for the functioning of the internet (like the root name servers outlined above).

> States may be able to improve international security by considering which systems should be considered off limits, like the root name servers.

Military transparency. The opportunity to set a new course on declaratory policy, transparency, and military-to-military cooperation should be considered in advance of a potential disruption such as that outlined in this scenario. Regional familiarization with military culture and doctrine around cyberspace operations would contribute to conflict management and de-escalation in the event of a conflict between China, the United States, and Vietnam, among others.

Cybersecurity investments and response options. In this scenario, the information technology infrastructure of CNOOC, the Vietnamese airport systems, the hospitals in Hanoi, and potentially the Great Firewall all rise to the level of infrastructure whose disruption may trigger national concern and response requirements. States across the region should identify their top-tier infrastructure, facilitate infrastructure security, and determine appropriate responses for levels of intrusion. In this scenario, China's surveillance and unintentional deployment of malware against Vietnam's hospital infrastructure was a disproportionate response to the Vietnamese hacktivist action on CNOOC's networks. A better option for China may have been to simply increase CNOOC's network defense capabilities and let the issue lie (raising the issue with Vietnam again if and when China needs an economic or political concession). Countries should consider thresholds internally to determine whether and how responses may be warranted, including the use of surveillance that could in itself increase tensions.

Critical infrastructure protection investments. A final outstanding question this scenario poses is the degree to which companies would be willing to invest in capabilities to protect the critical infrastructure that matters most for their stability and security. This is a question for investors and companies to consider within the broader framework of liability, investments, and legislation. Given the nature of vulnerabilities, companies and countries must identify where and how to invest to secure their most important systems in the event of conflict escalation.[129]

Escalation in the Pacific

KEY TAKEAWAYS

An escalation in cyberspace between Vietnam and China leads to unintended fatalities and draws the United States, China, and Vietnam into a diplomatic crisis. **Key drivers in this scenario include** the use of cyberspace weapons by Vietnamese nationalist hacktivists and Chinese actors; geopolitical tensions along the South China Sea; an unresolved dispute that triggers escalation; and differing views regarding the Law of Armed Conflict and the governance of cyberspace operations. Enduring questions about China's rise and influence in the Asia-Pacific region also underpin the scenario. Ultimately, the scenario affords state and non-state actors an opportunity to push for changes in their approach to social controls in China and the governance of cyberspace operations globally.

Cybersecurity policy and strategy choices. Domestically, the CCP would be wise to anticipate domestic activists conducting cyberspace operations against the state in the event that grievances trigger activist sentiments like those outlined in this scenario. Beyond economic policy changes during the crisis itself, what democratic-oriented political concessions can the CCP plan in advance to undercut frustrations like those outlined in this scenario? Following a Vietnamese cyberattack, what messages could the government use to contain nationalist sentiments that would urge a muscular response?

In addition, President Xi would need to affirm his nation's resolve while balancing long-term stability to avoid needless entanglements or escalation, as this incident could place his national objectives at risk. In matters of foreign and defense policy, this scenario highlights how states can plan for a range of cyberspace incidents that may arise and identify proportionate response options for deterrence that help maintain stability. What would be an appropriate Chinese response to the Vietnamese attack on CNOOC in this instance? Countries regularly conduct surveillance on a range of targets during periods of tension, including elements of the energy sector or civil sector, some of which may be needlessly escalatory, given the potential for unintended consequences. To avoid needless escalation, China and other states should work internally to analyze triggers that may warrant a response, and then identify a range of options to help achieve deterrence, from trade sanctions to indictments. Would it be sufficient to say, as President Obama did in 2014, "we will respond in a time, manner, and place of our choosing" followed by a modicum of action? Limited response options may have been his best course.

Internationally, in advance of such a scenario, the United States should consider which aspects of critical infrastructure, like hospitals or the global internet, should be deemed "off-limits" as a part of potential bilateral agreements regarding the governance of cyberspace operations. A scenario such as this one would afford the United States a significant opportunity to set terms for such an agreement. In the wake of such an event, the United States can also consider when and how to seek concessions from China on other issues.

SCENARIO 3

The Beijing Cyberconsensus

INTRODUCTION

This scenario considers how China's investments have the potential to transform Asia's internet landscape and re-shape relations between Beijing and the countries that use Chinese technologies to China's benefit. In addition to generating profit and achieving some of the broader trade and foreign policy goals that President Xi seeks through the Belt and Road Initiative, China has the potential to use its increasing influence to affect the nature of cybersecurity planning and technology development in the region through a mix of private-sector spending and government funding of large-scale digital infrastructure.

More specifically, this scenario explores how China could use its ICT investments to extend its influence across multiple facets of cyberspace, from the network layer to hand-held devices to cybersecurity policies for apps. China's technological influence would then give the government in Beijing additional political capital. For instance, it could leverage existing umbrella projects like the Belt and Road Initiative to guide the recipients of China's ICT investments into an internet and cybersecurity governance system that benefits China's economic interests. Technology could thus enable Chinese power, first through economic gain and second by deepening the nation's ties to governments and companies across the region.

The narrative presented here raises key questions as Asia comes online: who will develop strong cybersecurity standards, operating principles, and internet protocols for regional governments that have not yet made these decisions (and may lack the capacity to do so)? Will it be Asian technology giants, or their host governments? Or will it continue to be established players and global internet governance institutions based in the United States and Europe?

China will play a role in the articulation of cybersecurity policies to increase its influence. The question is, which course will China choose—and how will other countries respond?

KEY DRIVERS

There are a variety of key drivers affecting the outcomes in this scenario, including tensions between countries with significant access to technology and political power (i.e., China) and those without; the economic and security impacts of China's strategic goals and expanding technology investments on diverse Asian populations and governments; the role of multilateral organizations in managing cybersecurity risks, internet governance, and development as internet access expands in Asia; and the future of Asian national governing bodies and policies in shaping cyberpolicies and cybersecurity.

What incentives would Chinese companies have for influencing cybersecurity policies and data protection regimes? Revenue alone makes the Asian market appealing to Chinese businesses. In 2015, over-the-top (OTT) media and service applications like Netflix, Flipkart, and WhatsApp provided twice the revenue of global physical infrastructure companies and investments.[130] Asian ICT companies logically aim to move up the production chain and away from infrastructure to increase their revenue in the app and data market.

Yet there are strategic issues at stake also. The Belt and Road Initiative will connect China to Eurasia through overland and maritime links. It is reportedly one of President Xi Jinping's most important foreign policies. It aims to create an economic zone in Eurasia that would allow China to dominate regional trade and gain greater access to European markets. It will tie Chinese companies to markets across the region, facilitate the export of Chinese goods like steel and cement across Eurasia, and build lucrative Chinese infrastructure projects for countries across the world's largest landmass.[131] All of this makes the Belt and Road vital to President Xi and his supporters' long-term success.

Information and communications technologies play a part in the Belt and Road Initiative as well. Yet Chinese ICT companies have struggled in foreign markets for a range of reasons, including stringent privacy laws, particularly in strong states like Singapore. In 2014, for example, Singapore's Personal Data Protection Commission began investigating Xiaomi, one of China's leading smartphone manufacturers,[132] in light of the claim that data from Xiaomi's cloud messaging service on the RedMi 1S phone was being forwarded automatically to external servers for unclear reasons.[133] This raised privacy and security concerns for the Singaporean government.

Moscow
POLAND
Rotterdam
GERMANY
Duisberg
BELGIUM
FRANCE
Venice
ITALY
UKRAINE
Istanbul
Athens
KAZAKHSTAN
RUSSIA
Almaty
Bishkek
UZBEKISTAN
Urumqi
Horgos
Samarkand
Dushanbe
Teheran
IRAN
PAKISTAN
Lanzhou
Xi'an
Beijing
CHINA
Gwadar
Kolkata
INDIA
Beihai
Hanoi
Fuzhou
Quanzhou
Guangzhou
Zhanjiang
Haikou
DJIBOUTI
SRILANKA
Colombo
Kuala Lumpur
MALAYSIA
KENYA
Nairobi
Jakarta
INDONESIA
Belt and Road Initiative
Silk Road Economic Belt
Maritime Silk Road Initiative

The Singapore dispute shows how major Chinese ICT companies can clash with data protection regulations in foreign markets. Countries have accused Chinese companies of sending user data stored abroad back to the mainland,[134] as China's cybersecurity regulations require Chinese ICT companies to turn over user data to the Chinese government on demand.[135] The Chinese government also restricts companies in China from exporting data abroad,[136] yet in the Singapore case, Xiaomi was forced to move its data servers outside of China to comply with Singapore's privacy standards.[137] Given the Chinese government's policies, Chinese technology companies will continue to run into hurdles when faced with established data protection regulations in China and externally.

Lack of institutional capacity is a major driver as internet access expands and risk increases. Unlike Singapore, most emerging economies and country members of the Asian Infrastructure Investment Bank (AIIB) have yet to implement or articulate policies for protecting data and infrastructure (as the table on the following page illustrates). Chinese companies (and the Chinese government) thus have an opportunity to promote their own cybersecurity policies and influence the policies of Asian countries to their advantage when they can.[138] As Chinese companies expand into less-developed markets in Asia—including countries with limited to no national cybersecurity or data protection policies—they use their market influence to push for a "Beijing Cyberconsensus" that influences countries to make cybersecurity policy decisions favorable to China. Absent robust institutional capacity, China can easily step into other countries' processes to exert its influence.

Add to this equation the question of Asian device security. Unfortunately for China, from a cybersecurity standpoint, Chinese goods are often more vulnerable than hardware and software systems designed in other countries,[139] placing Asian users of Chinese technologies at greater risk. Consider one potential risk that multinational firms might face from more vulnerable goods. Electronic card giants like Visa and MasterCard provide end-to-end protection for digital payments through the Secure Electronic Transaction (SET) and 3D Secure Protocols. These protocols secure the user, but they are only as good as the security on the device itself, often a mobile phone or tablet. In Asian digital economies marked by the proliferation of cheap and insecure handheld devices, global corporations and users may face increased cyber-enabled financial fraud and other risks.

In an effort to address these and other security concerns, Asian countries will try to influence standard-setting institutions that can force corporations to improve their approach. One such regulatory body is the Internet Engineering Task Force (IETF), a multi-stakeholder body that sets internet standards and is dominated currently by the major internet and telecommunications corporations. The multinational nature of bodies like the IETF and the lack of standards in Asia thus provide China with an opportunity to shape technical standards and protocols in countries that do not yet have them (or to force countries to raise the issue within multilateral systems that could come to their aid). In a power struggle between China and lesser powers dependent on Chinese goods, like Laos or Kyrgyzstan, China will use its technological and economic heft to come out on top.

Table 2: Data protection norms and cybersecurity standards among AIIB (Asian Infrastructure Investment Bank) members

COUNTRY	Data Protection Norms (per ITU)	National Cybersecurity Standards (per ITU)	Member of AIIB
Afghanistan	NO	NO	NO
Azerbaijan	YES	YES	YES
Australia	YES	YES	YES
Bangladesh	NO	NO	YES
Brunei	NO	NO	YES
Cambodia	NO	NO	YES
China	YES	YES	YES
India	YES	YES	YES
Indonesia	YES	YES	YES
Japan	YES	YES	NO
Kazakhstan	YES	NO	YES
Kyrgyzstan	YES	NO	YES
Laos	NO	NO	NO
Malaysia	YES	YES	YES
Maldives	NO	NO	YES
Mongolia	YES	YES	YES
Myanmar	NO	NO	YES
Nepal	NO	NO	NO
Pakistan	NO	NO	YES
Philippines	YES	NO	YES
Singapore	YES	YES	YES
South Korea	YES	YES	YES
Sri Lanka	NO	NO	YES
Taiwan	YES	YES	NO
Tajikistan	YES	NO	YES
Thailand	YES	YES	YES
Turkmenistan	YES	NO	NO
Uzbekistan	YES	NO	YES
Vietnam	YES	NO	YES

Data drawn from International Telecommunications Union, "Cyberwellness Profiles," ITU, accessed August 23, 2017, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx

Finally, the Belt and Road Initiative will create a framework for policy coordination between China and partner countries[140] and provide political cover for Chinese companies and the Chinese government to push for its approach in South, Central, and Southeast Asia. Behind all of these ICT investments lies the possibility of China turning its ICT infrastructure into a platform to launch covert or overt cyberspace operations for military and intelligence purposes against Asian states and others. These drivers could combine and strengthen China's geostrategic position in matters of technological influence, foreign policy, and military power.

The Belt and Road Initiative will create a framework for policy coordination between China and partner countries.

SCENARIO

The year is 2020, and four countries have independently sought assistance from the Asian Infrastructure Investment Bank (AIIB) to strengthen the performance of their ICT sectors. Two of these countries, Tajikistan and Kyrgyzstan, are in Central Asia while the other two, Laos and Cambodia, are members of ASEAN. The four projects are worth $500 million each and aim primarily to strengthen the physical telecommunications and internet infrastructure of each country. The AIIB's Board of Governors, in line with their powers under the Bank's Articles of Agreement, decide unanimously to grant direct loans to the four applicants.[141] The Board is reluctant to impose conditions on the loans, but agrees that the requests for proposals and bidding process should be conducted in as transparent a manner as possible.

Following an exhaustive vetting process, a small group of companies succeed in bidding for all four projects. China Telecom wins contracts in Kyrgyzstan, Laos, and Cambodia to build telecommunication towers through a joint venture with the respective national carriers;[142] the Chinese company ZTE will lay the optical fiber transmission lines for all projects.[143] Looking to improve their mobile and broadband penetration rates—Cambodia is at 6%; Laos at 13%; Tajikistan at 16%; and Kyrgyzstan at 24%[144]—each government seeks tenders from mobile manufacturers that can offer affordable handsets to their populations. Huawei secures this tender through an attractive package that bundles together smartphones and routers for local internet carriers.[145]

Some member countries of the AIIB register a formal protest, alleging that the tender process was manipulated to favor Chinese companies. The investigation finds no evidence of wrongdoing.

Cambodia, Laos, Kyrgyzstan, and Tajikistan lack officially approved national or sector-specific cybersecurity frameworks, and this leaves them open to external influence.[146] Given their low rates of internet penetration and large-scale investments in physical telecommunications infrastructure by Chinese companies, the four countries begin to adopt—first in practice, and then by decree—domestic standards that are closely aligned to China's.

Chinese telecom and internet giants use this opportunity to mold regional technical standards and protocols in the region, starting with Tajikistan, Kyrgyzstan, Cambodia, and Laos, all members of the Belt and Road Initiative. Chinese companies argue that existing encryption standards, electronic payment protocols, and even internet routing protocols are ill-equipped for Asian economies, and call for an earnest dialogue to rewrite these rules regionally. Within a year, the Chinese government launches a multi-stakeholder initiative that aims to institutionalize cybersecurity policies, standards, and norms, co-opting AIIB members in the Asia-Pacific as well as Belt and Road destinations.

After successfully synchronizing national policies on connectivity and cybersecurity standards, a group of countries led by China begin negotiations to create regional internet governance institutions. The first such institution is a standard-setting body for encryption across devices and platforms, along the lines of the National Institute of Standards and Technology (NIST) in the United States. Based in Shanghai, the Asian Institute for Technology Standards (AITS) convenes a conference that brings together Belt and Road and AIIB member countries for a blue-skies discussion on the state of cybersecurity in Asia. Consensus emerges from this conference that many of the cybersecurity protocols and rules in the region need revisiting, and members sign on to an outcome document calling for the AITS to assume leadership in this matter.

As a result, China emerges as a norm entrepreneur, capable of influencing market behavior and strategic engagement between states and companies around digital issues. China and Chinese companies urge greater data protection measures for everyone. Yet in this scenario, China seeks to guarantee that companies and the government can maintain remote access to user devices to force security updates regardless of user preferences, and for companies to be able to de-encrypt a user's device in the case of a national security requirement. While China purports to protect user data, these initiatives de-emphasize privacy and intellectual property protections over ostensible state security requirements. Consequently, Chinese companies focus less on ensuring encryption across platforms for users, and more on developing endpoint security systems to track malicious attacks and abnormal behavior. China's focus on ensuring access to user information for national security influences other states, like Myanmar, Pakistan, Tajikistan, Cambodia, and Laos.[147]

Emerging economies in the Asia-Pacific may not accept this Beijing consensus of cybersecurity policies, standards, and technological investments, but many still have to contend with China's views given China's growing ICT influence in the region. Some countries may try to opt out by choosing alternative companies that provide a better mix of security and privacy. With their own technology sectors and stronger cybersecurity policies, India, Japan, Australia, Singapore, Vietnam, and South Korea opt to stay away from institutions like AITS and criticize China's efforts to disrupt current institutions for its own political and economic benefit.

Emerging economies in the Asia-Pacific may not accept this Beijing consensus of cybersecurity policies, standards, and technological investments.

POTENTIAL OUTCOMES

Chinese investment in ICT infrastructure across the Asia-Pacific region will have immediate political and market-related consequences. In an economy dominated by cheap and vulnerable devices, some regulators will feel compelled to guard against a culture of limited data protection, whether through China's dilution of legal standards related to data sharing, relaxation of security testing measures by hardware manufacturers, or the weakening of encryption protocols. This will manifest through regulatory battles in foreign courts between independent regulators and Chinese internet companies who may seek their own set of rules for the digital economy. At an institutional level, Asian economies will be wary of further tapping the AIIB's resources if it is perceived to favor Chinese interests over other competitors.

A regional schism in data and cybersecurity norms. As a result of cybersecurity choices by countries, Asia may see a divergence in data protection norms, with wealthier countries like Singapore, Australia, Japan, New Zealand, and South Korea imposing strong safeguards on the integrity of their users' data. At the same time, less wealthy counties may be compelled by the need to provide cost-effective infrastructure and may be forced to opt for weaker regulations.

The schism in data protection norms could fragment the digital ecosystem and place additional burdens on transnational ICT corporations as they try to navigate economies and jurisdictions in Asia. Countries with weaker cybersecurity standards and data protection norms would perpetuate a techno-class divide, with elites opting for expensive, sophisticated handheld devices that protect user privacy. Significant disruptions or theft against the less protected would lead to political pressures on state and national governments to bridge the class divide in cybersecurity protections.

First-generation internet users would continue to rely on cheaper devices that affect access to over-the-top services and applications, like WhatsApp, Netflix, Facebook, Flipkart, Alibaba, or GrabTaxi. They would be alarmed by the proliferation of malicious attacks on their low-end devices, which would discourage the use of applications that deal in personal information (like financial transactions). Faced with differing cybersecurity standards and data protection norms across the region, Computer Emergency Response Teams (CERTs) would be reluctant to share information with countries that follow China's cybersecurity approach, making the cross-border investigation and prosecution of cybercrimes more difficult. Foreign companies would be unlikely to use parts manufactured in the region, and Western institutions would resist placing data centers in Asia.

Loss of faith in multilateral forums and institutions. Nations that are members of the Asian Infrastructure Investment Bank, already skeptical of this institution as a vehicle to promote Chinese influence in the region, would begin to reconsider their association. Under the AIIB's Articles of Agreement, the Bank is "required to pay due regard to the desirability of avoiding a disproportionate amount of its resources being used for the benefit of any member."[148] Founder members would invoke this clause, claiming that the Bank's resources are being used to promote the creation of norms and architectures that go beyond the scope of project financing to favor Beijing.

Backlash against China. Over time, as Chinese companies fail to invest in cybersecurity, countries that once welcomed China's investments would find themselves pivoting away as cyberincidents build up. News headlines would decry "yet another ransomware attack" exploiting "yet another vulnerability in a Chinese product," discouraging government and industry leaders in countries that are dependent on China's technology or approach to governance.

In some cases, foreign law enforcement agencies would find it difficult to extract data from cloud services and app providers based in China, leading to some tensions in bilateral relations. Even as Chinese products infiltrate Asian markets, American, South Korean, Japanese, or Indian digital services and products firms would lobby for regulations to mitigate the anti-competitive effects of Chinese dominance.

Historical precedents already exist for such a response: in June 2017, Facebook filed a software patent in India for its WhatsApp-driven payment system, which if granted to Facebook would place limits on Chinese message-enabled payment platforms like WeChat that have yet to enter India.[149] The backlash against China's attempts to rewire the rules of cybersecurity or internet governance may therefore come from users, governments, and businesses alike. Consequently, Chinese companies, much like Xiaomi in Singapore in 2014, may set up data servers outside the Chinese mainland with a view toward catering to diverse market regulations. This would undermine Beijing's goal of harmonizing the region's digital regulations in its favor.

Cybersecurity market surprise. In an alternate outcome, China may buckle under pressure as countries reject its emphasis on granting access to encrypted devices. In this case, Chinese technology companies could make a concerted effort to leapfrog legacy ICT systems and invest in enhanced cybersecurity capabilities across the region to protect users. After investing for between two to five years, China could emerge as a cybersecurity leader and capture a wider portion of the Asian cybersecurity market in a manner that China has not yet achieved.

This outcome would still call into question states' preferences for Chinese goods and influence within their borders and on their populations, but an increased focus on cybersecurity products and services across Chinese technologies would improve the country's technological capabilities and therefore strengthen the allure of the Beijing Cyberconsensus as countries weigh whether to opt in or not.

CONCLUDING LESSONS FOR POLICY PLANNERS AND STAKEHOLDERS

This scenario presents an example of China making the shift from being a "norm taker" to a "norm entrepreneur" through the heft of its economic might and expanding geostrategic influence. By wiring the Asian ICT ecosystem through its pipes, tubes, towers, routers, and handheld devices, China influences the evolution of data-sharing regulations and agreements across digital infrastructure toward its own view of enforced security updates and guaranteed state access to encrypted devices. Such a scenario raises a series of questions for governments and industry—as well as regional policy planners and stakeholders—regarding China's potential cybersecurity capabilities and intent, and presents choices that countries can make now to maximize the benefits and minimize the risks of the Belt and Road Initiative and China's ICT investments.

Plan cybersecurity policies now to avoid giving Chinese companies and the People's Republic of China undue influence. As a supplier of digital infrastructure and networks in Asia, Chinese companies play a role in creating cybersecurity standards across the region. China's economic clout would give China potential *de facto* veto power over the creation of ICT policies in economies that are reliant on Chinese investment. For example, Asian governments keen to boost their internet connectivity would welcome more affordable services. Gradually, these platforms would create captive economies in Asia that run on Chinese digital technologies. Countries should plan now for cybersecurity standards and protocols to meet their population's needs and resist giving China (or any other country) undue influence.

States should decide now on their approach to key questions in encryption and remote access. On encryption, states should decide whether to sustain encryption in all cases, as opposed to decrypting data for a national security case. States should also determine their policies regarding state access to personal and corporate data, including protections for corporate intellectual property for companies operating within their borders. Finally, like Singapore, states should decide whether and how to address Chinese companies' requirements to store data in China or share data with the Chinese government.

Differentiate approaches to ICT trade and non-ICT trade. The Belt and Road Initiative was conceived as a mechanism to connect Chinese companies to European markets. According to the Chinese National Development and Reform Commission, the Belt and Road Initiative serves the goals of "policy coordination, facilities connectivity, unimpeded trade, financial integration, and people-to-people bonds."[150] In any 21st-century economy, these goals will be realized through digital conduits: payment gateways, distributed technologies for managing supply chains, common protocols to ensure machine interoperability, and social media platforms to facilitate communication. China's role as an indispensable player in the creation of digital ecosystems across Asia will help it become a stronger arbiter of regional and trans-continental trade. The success of trade facilitation agreements in particular would depend on Chinese infrastructure, which would in turn further enhance Beijing's strategic influence in the region.

Policy planners and investors should consider whether China's technology measures up from a security standpoint, but also whether and how to explore disaggregating ICT trade with China from broader trade and foreign policy goals. Should countries diversify their trade portfolios away from China to avoid giving China undue influence? What is the appropriate basket of investments for a country to consider, given cybersecurity risks and the costs of technology?

Recognize that expanding Chinese ICT infrastructure may lead to enhanced cyberspace operational capabilities. If China is building telecommunications infrastructure and ICT platforms in other countries, how can those countries ensure that China does not use that infrastructure to conduct cyberspace operations against a third party? Can countries that host Chinese ICT infrastructure and platforms negotiate a monitoring agreement to prevent certain kinds of traffic or data from passing through their infrastructure? What assurances can countries reasonably seek to gain from China regarding the use of Chinese telecommunications platforms for peaceful means? These are questions any country should consider as it procures ICT platforms through the Belt and Road Initiative or another Chinese investment process. In many instances, it may be impossible to pressure China to use ICT in any particular way, but it would be possible to push for norms and laws that govern the conduct of cyberspace operations.

To make decisions on these and other issues, countries should set up a cybersecurity vetting body similar to the United States' Committee for Foreign Investment in the United States (CFIUS), a U.S. government mechanism managed by the Treasury Department[151] that reviews the political and security implications of foreign investments for a country.

The Beijing Cyberconsensus

KEY TAKEAWAYS

As a part of the Belt and Road Initiative, China expands its ICT investments in Asia to shape the contours of cybersecurity over time by providing a physical infrastructure for an expanding internet and influencing how countries develop and implement their cyberpolicies.

Key drivers in the unfolding of the scenario include China's rising influence in economic and security policy; a lack of institutional control and expertise around cybersecurity in countries susceptible to China's influence; the gap between the technological "haves" and "have-nots"; the impact that the desire for technology and access may have on emerging economies; and Asia's deepening influence on the evolving internet in multilateral forums.

How might countries, companies, and multilateral organizations behave in the face of Chinese foreign direct investments and expanding influence? Some may seek to influence China's behavior to achieve mutually beneficial technical standards of security and investments; some may opt-into China's approach, depending on their economic and security status and broader geopolitical alignment; and some may opt out of China's dominance and choose to either develop their own products or procure services and products from other countries. Certainly the rise of China's economic and ICT influence will force countries to make strategic choices to balance their interests and protect their investments.

Cybersecurity policy and strategy choices. Policy considerations include initiating advanced planning for ICT security and standards to head-off China's influence before its ICT presence and investments expand; identifying how best to separate cybersecurity from other trade-related issues; and planning for China's potential operational capabilities as it expands its ICT infrastructure. Countries should begin to make changes to their cybersecurity policies to meet their most important interests first; i.e., are there some ICT capabilities in a country that should be judiciously protected against foreign influence and made robust, like key leader communications? Countries can begin now to make limited investments to get ahead of potential outside risks using some of the lessons that this scenario identifies.

CONCLUSION

Cybersecurity Opportunities in Rising Digital Asia

This study presents premises and drivers that will shape Asia's cybersecurity future, and then outlines storylines of cooperation, competition, and conflict in the region. Through scenarios, the study aims to take readers away from the "daily inbox" of perceptions and assumptions; to remove analytic constraints of the cybersecurity domain by bringing diverse socio-political forces together in narratives; and to suggest pathways for achieving resilience in matters of cybersecurity. Asia faces a range of potential future challenges as unaccustomed populations and governments face a rise in internet access and use, from interstate conflict to cyberattacks on diverse economic sectors, like agriculture. Given the coming rise of internet access and use in Asia, what opportunities exist for government and companies and citizens?

I. Unlike internet expansion in the West, where access and speed were the first priorities and security was largely an afterthought, Asia can shape its cybersecurity at an earlier stage in its internet growth. Asian corporations and governments can learn from the past and build cybersecurity into their societies before hundreds of millions of new users come online. In the first scenario, it is only after an incident that India develops a campaign to educate the country about cybersecurity best practices. Similarly, in the third scenario, if China makes cybersecurity a key part of its ICT investments in the Belt and Road Initiative, it becomes an effective regional cybersecurity service provider for countries across the region. Yet these benefits need not wait for new storylines, as India and China can pursue both objectives today.

A range of opportunities exist at this early chapter in Asia's internet build-out. Network and application developers can incorporate cybersecurity technologies into their projects now; public and private-sector leaders can shape cybersecurity policies and standards by advocating for change within their countries; and major Asian markets can influence global ICT companies to improve their cybersecurity practices to meet their populations' needs. From incorporating encryption to building redundant networks to developing national education campaigns, countries and companies can deploy a variety of solutions to help secure the region. Small and early investments in personnel and key strategic goals can help countries get ahead.

II. At this stage in Asia's internet expansion, strategic planning and analysis can have a profound and positive impact on the future of the region—and present an opportunity for leaders to effect change across societies. Rather than acting piecemeal, strategic planners can take a comprehensive approach, examining risks and opportunities in cybersecurity and imagining the future that they would like to build. Strategies can focus on identifying gaps in Asia's cybersecurity and where to invest to implement change. A modicum of investment and strategic planning can help close vital policy and security gaps; this study surfaced early priorities, including:

- *Identify clear roles and missions for agencies and companies.* This includes identifying key cybersecurity missions between and among sectors and government agencies; workforce development and allocation; and public-private cooperation and information sharing, with a focus on high-risk sectors like national security, energy, finance, and public health.

- *Prioritize protecting the data that matters most.* This involves applying scarce cybersecurity resources judiciously to mitigate the most important risks. For prudent planning, countries can identify the infrastructures that would lead to significant national consequences if disrupted through cyber means (beginning again with national security, energy, finance, and health). Absent this information, resource prioritization may be impossible to achieve.[152]

- *Get the cybersecurity basics right.* Countries and organizations can initiate cyberhygiene campaigns now to make societies more secure, beginning with simple campaigns (i.e., popular education about counter-phishing, two-factor authentication, and strong passwords).

- *Design proportional responses to cyberincidents.* In matters of foreign and defense policy, governments can think through measured, proportional response options for cyberattacks that emanate from abroad. Key questions include: How might an intrusion be perceived as a potential escalation? What cyber or non-cyber responses would be warranted (or not)? Where should countries invest to build capabilities? Scenario-based exercises can help reveal gaps, seams, and capability deficiencies and set companies and countries on a better course.

- *Conduct advanced planning.* As a part of the process of developing norms, governments can decide whether to designate select targets as off limits for cyberreconnaissance or cyberattack. Potential proscriptions might include the SWIFT code system, the root name server, or data systems of public health. Bilateral agreements between countries on these points will not eliminate all risks (as there will always be the chance of non-compliance, accidents, or the actions of third parties, like terrorists), but will reduce them. To seize opportunities, states should make decisions in advance regarding potential policy goals they would like to achieve, along with proposals they could present to other countries.

- *Implement risk assessment measures.* If they have not yet done so, governments can design mechanisms for assessing the security risks of foreign technological investments and ask: Why are countries building a specific ICT globally or in our country? If a technology is being introduced into a country, what controls can be put in place to protect populations? Decisions on ICT should include security and economic aspects.

III. Every organization should plan and exercise to perform its critical missions and functions without assured access to secure data. "Cyberspace is not a target in itself," as one specialist said, "It's a medium." The internet connects hackers to targets across human society.[153] Attackers will use cyberspace to disrupt critical missions for their own advantage; geopolitically, attacks can be anticipated during periods of tension, to include escalating conflicts between states, political elections, or moments of change when a state or community is vulnerable to manipulation. For maximum impact, astute attackers will target centers of gravity like those outlined in this study—the finance, energy, and public health sectors; military operations; and the operations of political organizations and campaigns.

As the internet expands in Asia and populations become increasingly dependent upon it at the political and technical level, nothing may matter more than building resiliency to withstand potential disruptions. Governments and militaries can build emergency communications to continue national security and public safety operations without interruption. Every organization can build redundant data storage and back-up capabilities to protect the most important data. In politics, political and media leaders should prepare for manipulations like the campaign Russia conducted during the 2016 U.S. election. Technology companies are working now to address the risks associated with the proliferation of online propaganda (i.e. fake news) and online echo chambers. Good leadership, reasoned and inclusive political rhetoric that focuses on the well-being of the whole, and a just rule of law that protects all citizens and allows for dissent can help undercut extreme political narratives that make cyberspace operations an attractive tool to would-be attackers.[154] In rising digital Asia, it is not a question of if but when attacks and disruptions will come. Countries have a moment of opportunity to build resilience at the technological and political level. Scenario thinking and strategy development can help organizations to see the way forward.

This study presents potential cybersecurity storylines for one of the world's most dynamic economic regions. Countries across the Asia-Pacific have gone from agrarian societies to emerging economies to near middle-income status in less than a generation. As we look to the future of cybersecurity in Asia, it may be impossible to predict how a society will adapt and evolve as technology exerts its influence, but we can look at how trends and drivers might interact over time—and thus imagine scenarios and prepare for an uncertain future. No matter what new technology may emerge, good leadership and advance planning can help society withstand any disruption and successfully manage change.

About the Authors

Jonathan Reiber is Senior Advisor at Technology for Global Security, a think-do tank based in Palo Alto, California, and a Visiting Scholar at UC Berkeley's Center for Long-Term Cybersecurity, where he previously held a two-year writing and research senior fellowship from 2015–2017. Prior to his appointment at Berkeley, Jonathan held a number of positions in the Obama Administration within the U.S. Department of Defense. In his last position, he served as Chief Strategy Officer for Cyber Policy in the Office of the Secretary of Defense, where he advised the Pentagon leadership and led initiatives across the cyberpolicy portfolio, to include strategic planning; key interagency and industry partnerships; and strategic communications. He was the principal author of *The Department of Defense Cyber Strategy* (2015). He also held a leadership role on the Department of Defense Task Force on Cyber Deterrence, and led delegations advising foreign governments in the Middle East on the formulation of cyberdefense policies and strategies. Earlier in the Obama Administration, Jonathan served as Special Assistant and Speechwriter to the United States' Deputy Secretary of Defense, Dr. Ashton B. Carter, and previously as Special Assistant to the United States' Principal Deputy Under Secretary of Defense for Policy, Dr. James N. Miller. In both positions he focused his work on foreign and defense policy, grand strategy, Middle East and Asia-Pacific affairs, and cybersecurity. Jonathan is a graduate of Middlebury College, where he studied religion and creative writing, and The Fletcher School of Law and Diplomacy, where he served as Editor-in-Chief of *The Fletcher Forum of World Affairs*. A former Thomas J. Watson Fellow, he is a regular advisor to governments and corporations on risk management, strategic planning, and cybersecurity, and his writing has appeared in *Foreign Policy, The Christian Science Monitor, The San Jose Mercury News, Mint*, and *Literary Hub* among others.

Arun Mohan Sukumar is a doctoral candidate at the Fletcher School of Law and Diplomacy, Tufts University. He is currently on leave from the Observer Research Foundation in New Delhi, where he headed its Cyber Initiative (2015–17). Arun is a member of the multi-stakeholder group set up by India's National Security Advisor to recommend policy and strategy for the promotion and negotiation of cyber norms. By invitation from the UN Institute for Disarmament Research (UNIDIR), Arun served as an independent legal expert in 2016 to the United Nations Group of Governmental Experts (UNGGE), the intergovernmental forum tasked with conceiving cyber norms, and to the UN First Committee on disarmament and international security in 2017. As its outgoing, elected Vice Chair, Arun completed a two-year term as one of the stewards of the Asia-Pacific Regional Internet Governance Forum. During the 2016 Tallinn Manual 2.0 consultations on the international law applicable to cyber operations, he joined the Indian delegation as its non-governmental representative. Arun is a member of the World Economic Forum's Global Future Council on the Digital Economy and Society. A lawyer by training, he has previously served on the editorial board of *The Hindu*, one of India's largest dailies. He holds a Master's degree from The Fletcher School of Law and Diplomacy, where he was the C. Douglas Dillon Fellow and the recipient of the Leo Gross Prize for Outstanding Student of International Law.

Endnotes

[1] "Internet Live Stats," InternetLiveStats.com, accessed August 17, 2017, http://www.internetlivestats.com. Internet Live Stats is a constantly updating website of Internet statistics compiling data from the International Telecommunications Union, the World Bank Group, and the United Nations Population Division (UNDP).

[2] For background on the South China Sea Dispute, see PCA Case number 2013–19, *In the Matter of the South China Sea Arbitration Before An Arbitral Tribunal Constituted Under Annex VII to the 1982 United Nations Convention on the Law of the Sea, Between the Republic of the Philippines and The People's Republic of China*, accessed June 14, 2017, https://pca-cpa.org/wp-content/uploads/sites/175/2016/07/PH-CN-20160712-Award.pdf.

[3] See U.S. National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington, D.C.: Office of the Director of National Intelligence, 2012), iv, https://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf.

[4] See World Bank, "Gross Domestic Product Ranking Table Based on Purchasing Power Parity (PPP)," *WorldBank.org*, accessed June 7, 2017, http://data.worldbank.org/data-catalog/GDP-PPP-based-table.

[5] For a long treatment on the role of telecommunications infrastructure in Asia's emergence and integration into the global economy, see the first few chapters of Thomas L. Friedman, *The World Is Flat 3.0: A Brief History of the 21st Century* (New York: Farrar, Strauss, and Giroux, 2007).

[6] For a list of the world's unicorn companies, see CB Insights, "The Unicorn List: Current Private Companies Valued at $1B And Above," *CBInsights.com*, accessed September 19, 2016, https://www.cbinsights.com/research-unicorn-companies.

[7] *Id.*

[8] See Internet World Stats, "Internet World Stats, Population and Usage," *internetworldstats.com*, accessed September 19, 2016, http://www.internetworldstats.com/top20.htm.

[9] Facebook page of Mark Zuckerberg, *Facebook.com*, last modified June 27, 2017, https://www.facebook.com/zuck/posts/10103831654565331.

[10] See Asian Development Bank, "Innovating Asia: Advancing the Knowledge Based Economy: The Next Policy Agenda," *Asian Development Bank*, accessed August 30, 2016, https://www.adb.org/sites/default/files/publication/59587/innovative-asia-knowledge-based-economy-pa.pdf. For further background on regional ICT investments, see also Digital India, "Digital India Initiative," *Government of India*, accessed September 19, 2016, http://www.digitalindia.gov.in; Infocomm Development Authority of Singapore, "Singapore's 'Smart Nation' Initiative," *Government of Singapore*, accessed September 19, 2016, http://www.ida.gov.sg/Tech-Scene-News/Smart-Nation-Vision. For an excellent treatment on the Internet's role in economic growth in India today, see also James Crabtree, "India Internet: Laying the Foundations," *The Financial Times*, January 20, 2016, https://www.ft.com/content/d9456e08-ba23-11e5-bf7e-8a339b6f2164.

11
U.S. Department of Justice, “Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector,” *U.S. Department of Justice*, accessed June 1, 2017, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

12
U.S. Director of National Intelligence, “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution,” *U.S. Director of National Intelligence*, accessed May 10, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

13
U.S. Department of Commerce, Census Bureau, Economic Indicators Division, “Top U.S. Trade Partners Ranked by 2016 U.S. Total Export Value for Goods (in millions of U.S. dollars),” *U.S. Department of Commerce*, accessed July 12, 2017, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_003364.pdf.

14
For reporting on the Bangladesh Central Bank cyberattack, see Nicole Perloth and Michael Corkerey, “North Korea Linked to Digital Attacks on Global Banks,” *The New York Times,* September 12, 2016, http://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html?_r=1. See also an in-depth Reuters report on the subject, Krishna N. Das and Jonathan Spicer, “How the New York Fed Fumbled Over the Bangladesh Bank Cyber-Heist,” *Reuters*, July 10, 2017, http://www.reuters.com/investigates/special-report/cyber-heist-federal/. While the theft apparently originated through the exploitation of vulnerabilities in the Bangladesh Central Bank (including apparently a lack of a firewall and second-rate switches), the Reuters article also reports that the New York Fed failed to respond to unanswered SWIFT messages from the Bangladesh Federal Reserve in a timely manner. The hack is illustrative not only of the risks facing global financial institutions from cybersecurity vulnerabilities and poor cybersecurity practices, but also of the necessity of back-up communications systems in the event that systems are disrupted by electronic means, as the SWIFT system was in this case. Per this report, the Bangladesh central bank also did not have direct phone numbers or emails to reach New York Federal Reserve personnel outside of New York business hours, and bank personnel instead used email and phone numbers listed on the Fed web page. At the same time, the New York Federal Reserve was slow to reach out to the Bangladesh Central Bank when SWIFT messages went unanswered. If these facts are correct, they point towards the need for (1) business continuity plans that can put key leaders in touch in rapid order; (2) the need for redundant lines of communication to facilitate the resolution of cyber-enabled financial issues if the SWIFT system is down, as it was in Bangladesh.

15
Ash Carter, “The Rebalance and Asia-Pacific Security: Building a Principled Security Network,” *Foreign Affairs* (November/December 2016), https://www.foreignaffairs.com/articles/united-states/2016-10-17/rebalance-and-asia-pacific-security.

16
Naazneen H. Barma, Brent Durbin, Eric Lorber, and Rachel E. Whitlark, “‘Imagining a World in Which’: Using Scenarios in Political Science,” *International Studies Perspectives* 17 (2016): 119.

17
See U.S. National Intelligence Council, “Global Trends: Paradox of Progress,” *Office of the Director of National Intelligence*, accessed August 17, 2017, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf.

18
For background on U.S. Defense Department planning and scenarios, see *inter alia* Martin Neil, Wade Hinkle, and Gary Morgan, “Scenarios—International Best Practice: An Analysis of Their Use by the United States, United Kingdom, and Republic of Korea,” *Institute for Defense Analysis*, August 17, 2017, https://www.ida.org/idamedia/Corporate/Files/Publications/IDA_Documents/SFRD/2016/D-5665.pdf.

[19] The story was told to one of the authors at a White House forum in 2010.

[20] Center for Long-Term Cybersecurity, *Cybersecurity Futures 2020* (Berkeley: Center for Long-Term Cybersecurity, 2016), accessed September 20, 2016, https://cltc.berkeley.edu/scenarios.

[21] On the limits of predictive modeling and scenarios for anticipating shocks, see Richard Danzig, "Driving in the Dark: Ten Propositions about Prediction and National Security," *Center for New American Security*, accessed September 19, 2016, https://www.cnas.org/publications/reports/driving-in-the-dark-ten-propositions-about-prediction-and-national-security; see also Phillip Tetlock, *Expert Political Judgment: How Good Is It? How Can We Know?* (Princeton, NJ: Princeton University Press, 2005).

[22] Leisha Chi, "Asian Companies Have the World's Worst Cybersecurity Says Study," *BBC.com*, August 26, 2016, http://www.bbc.com/news/technology-37163076. For background on global cybersecurity firms and their development, see Markets and Markets, "Cyber Security Market by Solutions (IAM, Encryption, DLP, UTM, Antivirus/Antimalware, Firewall, IDS/IPS, Disaster Recovery), Services, Security Type, Deployment Mode, Organization Size, Vertical & Region—Global Forecast to 2021," *Markets and Markets*, accessed September 5, 2016, http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html. According to the report summary, the global cybersecurity market is projected to grow from $122 billion in 2016 to $202 billion by 2021, at a compound annual growth rate of 10.6 percent.

[23] Rieko Arashi, Catherine Cloud, et al., "Asia-Pacific Defense Outlook 2016: Defense in Four Domains," Deloitte White Paper, accessed August 1, 2017, https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/public-sector/gv/en-gv-ap-defense-outlook-2016-160216.pdf.

[24] There have been a number of policy statements regarding the U.S. rebalance to Asia. The former U.S. Secretary of Dense Ashton B. Carter was one of the most vocal supporters and implementers of the rebalance, and delivered a number of speeches on the subject. See for example: Ashton B. Carter, "Remarks on the Next Phase of the U.S. Rebalance to the Asia-Pacific (April 6, 2015)," (speech, McCain Institute, Arizona State University, Tempe, AZ, April 6, 2015), http://www.defense.gov/News/Speeches/Speech-View/Article/606660/remarks-on-the-next-phase-of-the-us-rebalance-to-the-asia-pacific-mccain-instit.

[25] For more on the rebalance and its successes and failures, see Michael H. Fuchs, "Obama's Asia Pivot Has Been a Historic Success," *The New Republic*, August 31, 2016, https://newrepublic.com/article/136432/obamas-asia-pivot-historic-success.

[26] Outside of China's rise, which is a long-term challenge for the region and the globe, nuclear-armed North Korea presents a real and present threat to regional and global stability. In addition to its conventional weapons, North Korea has not only invested in cyberspace capabilities but displayed a willingness to use cyberspace operations on at least two occasions, including a hack of South Korea's banking systems and the American subsidiary of Sony Pictures Entertainment.

[27] "China's Internet: A Giant Cage," *The Economist*, April 6, 2013, http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled.

[28] "What is China's Belt and Road Initiative?" *The Economist,* May 15, 2017, https://www.economist.com/blogs/economist-explains/2017/05/economist-explains-11.

29
"GRIZZLY STEPPE—Russian Malicious Cyber Activity," *U.S. Department of Homeland Security* and *Federal Bureau of Investigation*, accessed May 26, 2017, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20 STEPPE-2016-1229.pdf.

30
A review of regional strategies and literature indicates that Australia, China, Indonesia, Burma, North Korea, Singapore, South Korea, Thailand, Japan, and Vietnam have all either invested or declared their intention to invest in military cybersecurity forces for defensive purposes to varying degrees. Many investments may not be publicly discussed. See U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2016," *U.S. Department of Defense*, accessed February 7, 2017, https://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20 Military%20Power%20Report.pdf. For background on these countries, see the national cybersecurity strategies listed on the webpage of the NATO Cooperative Cyber Defence Center of Excellence, "Cyber Security Strategy Documents," *NATO Cooperative Cyber Defence Centre of Excellence*, accessed June 14, 2017, https://ccdcoe.org/strategies-policies.html. For a broader overview of countries across the region, see International Cyber Policy Centre, "Cyber Maturity in the Asia-Pacific Region," *Australian Strategic Policy Institute*, accessed June 14, 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ASPI-Cyber-Maturity-2016.pdf.

A review of national strategies and events indicates that Australia, China, North Korea, South Korea, and Thailand have declared their intent to invest in capabilities to conduct offensive cyberspace operations, as well as, in some cases, defensive capabilities to counter an incoming cyberattack. Due to the technical nature of such operations, the line between offensive operations (to disrupt an adversarial system to terminate or affect a conflict on terms favorable to the offensive party) and counter-offensive operations (to defend a country against incoming attack by blunting or stopping an incoming attack) are often largely a question of intent.

For writing on Australia's offensive investments, see Government of Australia, Australia's Cyber Security Strategy, First Annual Update, 2017 (Canberra: Government of Australia, 2017), 15. For additional background on China, see China, China Military Strategy, May 2015, accessed November 14, 2017, https://news.usni.org/2015/05/26/document-chinas-military-strategy, and Shannon Tiezzi, "China Finally Admits to Hacking," *The Diplomat*, June 14, 2017, http://thediplomat.com/2015/03/china-finally-admits-to-hacking. For South Korea, see Zachary Keck, "South Korea Seeks Offensive Cyber Capabilities," *The Diplomat*, Oct 11, 2014, https://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/, and "Cyber Maturity in the Asia-Pacific Region," *supra*, at 68. For North Korea, see Jimmy Jun, Scott Laroy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Responses," Center for Strategic and International Studies, November 23, 2015, https://www.csis.org/analysis/executive-summary-north-koreas-cyber-operations-strategy-and-responses. For Thailand, see coverage of the Thai Ministry of Defence declarations on cyber strategy and deterrence, Jittip Mongkolnchaiarunya, "The Trouble With Thailand's Cyber Approach," *The Diplomat*, August 4, 2016, http://thediplomat.com/2016/08/the-trouble-with-thailands-new-cyber-approach.

31
For recent statements on the applicability of the law of armed conflict to cyberspace operations, see *The U.S. Department of Defense Law of War Manual*, which states that, "Specific law of war rules may apply to cyber operations, even though those rules were developed before cyber operations were possible. When no more specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during cyber operations in armed conflict." U.S. Department of Defense, *Law of War Manual* (Washington, D.C.: U.S. Department of Defense, June 2015), 996, http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf.

The Geneva Conventions of 1949 furthered some of the most important principals of the law of armed conflict, particularly in terms of their distinctions between lawful combatants, noncombatants, and unlawful combatants. See the Geneva Conventions of 1949 and Additional Protocols, and their Commentaries, available at: International Committee of the Red Cross, "Treaties, States Parties and Commentaries," *International Committee of the Red Cross*, accessed September 18, 2016, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp.

32
While the International Code of Conduct offers that states should follow public international law in dealing with conflict in cyberspace, it is not explicit about the Law of Armed Conflict; instead, it focuses principally on Shanghai Cooperation

Organization-driven narrative on territorial integrity and sovereignty. See "International Code of Conduct for Information Security," Annex to letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Secretary-General, United Nations General Assembly, Sixty-Sixth Session, accessed September 20, 2016, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

The United States and China have found some areas of agreement in this space. In 2015, a United Nations-convened group of governmental experts—including representatives from China and the United States—submitted a document to the United Nations General Assembly arguing that aspects of critical infrastructure that contribute to public safety should be offlimits during conflict. The report states that "[a] state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." See "The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, Seventieth Session, Item 93, July 22, 2015, accessed September 18, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

This expert report is however a non-legally binding opinion—and as Jack Goldsmith says, "it's more an expression of hope than of limitation." Jack Goldsmith, "Don't Get Too Excited About A US-China Arms Control Agreement for Cyber," *Lawfare*, September 21, 2015, https://www.lawfareblog.com/dont-get-too-excited-about-us-china-arms-control-agreement-cyber. But norms pave the way for additional agreements. After the report's publication, the United States and China reportedly sought to agree bilaterally to a norm against targeting critical infrastructure during peacetime. See David Sanger, "U.S. and China Seek Arms Deal for Cyberspace," *New York Times,* September 19, 2015, http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?_r=1. Near the end of the Obama Administration, the United States and China then agreed to refrain from conducting cyber-enabled intellectual property theft "with the intent of providing competitive advantages to companies or commercial sectors" and to study avenues for agreement on norms of behavior in cyberspace. See White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," *White House*, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Finally, the G7 in April of 2017 affirmed the norms put forth by the UNGGE in a joint communiqué. As a norm to which states have agreed to support in principal, the UNGGE could lay the groundwork for future bilateral or multilateral agreements regarding the use of force against critical infrastructure, building off of the Geneva Convention. See G7 Foreign Ministers at Lucca, "G7 Declaration of Responsible States Behavior in Cyberspace," G7 Information Centre, April 11, 2017, http://www.g8.utoronto.ca/foreign/170411-cyberspace.html. At the right moment, these developments can lay the groundwork for potential future agreements regarding potential targets that may be offlimits during a conflict, such as those outlined in scenario two, *Escalation in the Pacific*.

33
U.S. Department of Justice, "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities," Press Release, U.S. Department of Justice, U.S. Attorney's Office, Southern District of New York, accessed September 19, 2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated. For the full Southern District of New York indictment, see United States of America vs. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, and Nader Saedi, U.S. Department of Justice, U.S. Attorney's Office, Southern District of New York, accessed September 19, 2016, https://www.justice.gov/usao-sdny/file/835061/download.

34
Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/. For Russia's activities in Georgia, see also Richard Andres, "Cyber-Gang Warfare: State-Sponsored Militias are Coming to a Server Near You," *Foreign Policy*, February 12, 2013, http://foreignpolicy.com/2013/02/12/cyber-gang-warfare/.

35
See the United States of America vs. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Go Chunhui, Criminal Number 14-118, U.S. District Court, Western District of Pennsylvania, May 1, 2014, https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

36
See Krishna N. Das and Jonathan Spicer, "How the New York Fed Fumbled Over the Bangladesh Bank Cyber-Heist," *Reuters,* July 21, 2016, http://www.reuters.com/investigates/special-report/cyber-heist-federal/.

37
See David Sanger, Nicole Perlroth, and Michael Schmidt, "Obama Vows a Response to Cyberattack on Sony," *The New York Times*, December 19, 2014, https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0.

38
See Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," *SANS Industrial Control Systems*, March 18, 2016, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

39
See Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

40
The best analysis of the Stuxnet virus and its capabilities comes from the computer scientist and security specialist Ralph Langner. For a detailed analysis of the malware used in the attack, how and why it worked, and how to prevent such attacks from succeeding in the future, see Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," The Langner Group, November 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

41
U.S. Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," *U.S. Director of National Intelligence*, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

42
Id.

43
See Maggie Penman and Ahmad Omar, "Obama Announces Sanctions Against Russia In Response to Alleged Hacking," National Public Radio, December 29, 2016, http://www.npr.org/sections/thetwo-way/2016/12/29/507430861/u-s-retaliates-against-russia-over-cyberattacks.

44
See Jose Pagliery, "The Inside Story of the Biggest Hack in History," *CNN Tech*, August 5, 2015, http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

45
For U.S. government policy on this matter, see U.S. Department of Defense, *The DoD Cyber Strategy* (Washington, D.C.: U.S. Department of Defense, April 2015), 10, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. Since its publication in 2015, the DoD cyber strategy remains one of the clearest statements of U.S. public policy regarding cyberdeterrence. For coverage of the strategy, see the *New York Times* editorial,

"Preparing for Warfare in Cyberspace," April 28, 2015, https://www.nytimes.com/2015/04/28/opinion/preparing-for-warfare-in-cyberspace.html and David Sanger, "Pentagon Announces New Strategy for Cyberwarfare," April 23, 2015, https://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html?mcubz=1. The short statement of deterrence policy outlined in the DoD Cyber Strategy was bolstered and strengthened significantly by recommendations in the Defense Science Board Task Force study on cyber deterrence released in the spring of 2017. For that report, see U.S. Department of Defense, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence," *U.S. Department of Defense*, February 23, 2017, https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller_03-02-17.pdf.

46
See the *DOD Cyber Strategy*, *supra* note 45, for background on formal government policy statements on when and how response decisions are determined.

47
See Ravi Kanbur, Changyong Rhee, and Juzhong Zhuang, eds., *Inequality in Asia and the Pacific: Trends, Drivers, and Policy Implications*, (Asian Development Bank; London and New York: Routledge, 2014), https://www.adb.org/sites/default/files/publication/41630/inequality-asia-and-pacific.pdf.

48
One notable example of this theory can be found in the popular rejection of the Baharat Jayanta Party in 2011 and the rejection of the Congress Party for that reason and others in 2014.

49
See, for example, Katsushi Imai and Bilal Malaeb, "Asia's Rural-Urban Disparity in the Context of Growing Income Inequality," Discussion Paper, Research Institute for Economics and Business Administration, Kobe University, August 18, 2016, http://www.rieb.kobe-u.ac.jp/academic/ra/dp/English/DP2016-29.pdf.

50
See Ronald Inglehart and Pippa Norris, "Trump, Brexit, and the Rise of Populism: Economic Have-Nots and Cultural Backlash," Faculty Research Working Paper, Harvard Kennedy School, August 2016, https://research.hks.harvard.edu/publications/getFile.aspx?Id=1401.

51
See BBC, "Kashmir: Why India and Pakistan Fight Over It," *BBC.com*, November 20, 2016, http://www.bbc.com/news/10537286.

52
For background on the Doka La crossing dispute, see Steve Lee Beyers, Ellen Barry, and Max Fisher, "How India and China Have Come to the Brink Over a Mountain Pass," *New York Times*, July 26, 2017, https://www.nytimes.com/2017/07/26/world/asia/dolam-plateau-china-india-bhutan.html?mcubz=1.

53
For background on China and India's border disputes, see Ralph Jennings, "China's Three Worst Border Disputes—and its Best Border Buddy," *Forbes,* July 27, 2017, https://www.forbes.com/sites/ralphjennings/2017/07/27/chinas-3-worst-border-disputes-and-its-best-border-buddy/#6a00c1f64f36.

54
See Lyle J. Morris, "The New 'Normal' in the East China Sea," *The Diplomat,* February 24, 2017, http://thediplomat.com/2017/02/the-new-normal-in-the-east-china-sea/.

55
Immanuel Wallerstein, *The Modern World-System: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century* (New York: Academic Press, 1976), 229-233, https://thebasebk.org/wp-content/uploads/2013/08/The-Modern-World-System.pdf.

56
For a short review of the role of nationalism in China and the CCP today, see John Richardson Cookson, "The Real Threat of Chinese Nationalism," *The National Interest,* August 28, 2015, http://nationalinterest.org/blog/the-buzz/the-real-threat-chinese-nationalism-13729. Nationalism should not be considered a monolithic force in any context; what matters is how it is fomented and used. As Cookson wrote in 2015 about President Xi, "No force has been more important in Xi's power grab than nationalism. He has presided over a country that has stoked patriotic fervor as well as antagonized its neighbors and the United States. The most immediate result of stirring up national sentiment has been to strengthen Xi's power within the seven-member Politburo Standing Committee." The expression of his consolidation is covered further in the scenario in this report, *Escalation in the Pacific*. For writing about young people and online expressions of nationalism online in China, see Lotus Ruan, "The New Face of Chinese Nationalism," *Foreign Policy,* August 25, 2016, http://foreignpolicy.com/2016/08/25/the-new-face-of-chinese-nationalism/.

57
For background on the rise of nationalism and violence in India, see Supriya Nair, "The Meaning of India's 'Beef Lynchings,'" *The Atlantic,* July 24, 2017, https://www.theatlantic.com/international/archive/2017/07/india-modi-beef-lynching-muslim-partition/533739/.

58
Cass Sunstein, *Republic.Com 2.0* (Princeton, N.J.: Princeton University Press, 2007).

59
Id.

60
Mark Ward, "Celebrating 40 Years of the Net," *BBC News*, October 29, 2009, http://news.bbc.co.uk/1/hi/technology/8331253.stm.

61
Internet Assigned Numbers Authority, "About," iana.org, accessed August 17, 2017, https://www.iana.org/about.

62
"World Agricultural Equipment Market, Agricultural Machinery Demand to Rise 6.7% Annually Through 2016," *PR Newswire*, July 2, 2012, http://www.prnewswire.com/news-releases/world-agricultural-equipment-market-agricultural-machinery-demand-to-rise-67-annually-through-2016-161042685.html.

63
See generally Philippe Jeanneax, "Digital Agriculture: The End of the Farmer's Decision-Making?," paper prepared for the SDSC Chair—UMR INRA SAD-APT Seminar 'Changes in Sustainable Organization and Food Sector Management: Technical and Organizational innovations and Contractualization', Paris, France, June 1–2, 2017, http://www.chaire-sdsc.org/IMG/pdf/170518_jeanneaux_agrinum_fullpaper_sdscseminar_062017_cle81fdd7-1.pdf.

64
Id.

65
Sam Byford, "DJI Announces $15,000 Agricultural Drone Designed to Spray Crops," *The Verge,* November 26, 2015, http://www.theverge.com/2015/11/26/9805778/dji-agriculture-drone-agras-mg-1; IQI, "Smart Farming: How digital technologies

make farming more efficient," IQI, last modified November 10, 2015, http://www.i-q-i.net/de/smart-farming-wie-digitale-technologien-die-landwirtschaft-effizienter-machen/.

66
Carsten Dierig, "Wir Sind Besser Als Google," *Gründerszene,* last modified November 9, 2015, http://www.gruenderszene.de/allgemein/baywa-smart-farming-google?utm_source=newsletter&utm_medium=newsletter&utm_campaign=daily&utm_term=baywa-smart-farming-google&utm_date=2015-11-10.

67
Michel Lev-Ram, "What John Deere is Doing to Fight Slumping Sales," *Fortune,* November 15, 2015, http://fortune.com/2015/11/15/john-deere-software-services-agriculture-data/.

68
Prachi Salve, "How Many Farmers Does India Really Have?," *Hindustan Times,* August 11, 2014, http://www.hindustantimes.com/india/how-many-farmers-does-india-really-have/story-431phtct5O9xZSjEr6HODJ.html.

69
Kim Arora, "Only 9% of Rural India has Access to Mobile Internet: Report," *Gadgets Now*, February 3, 2016, http://www.gadgetsnow.com/tech-news/Only-9-of-rural-India-has-access-to-mobile-internet-Report/articleshow/50840296.cms.

70
See generally James Manyika et al., *The Internet of Things: Mapping the Value Beyond the Hype* (McKinsey Global Institute, June 2015), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

71
The most severe IoT-enabled attack recorded through October 2017 was the targeting of Domain Name Service (DNS) provider Dyn through connected devices like webcams, digital cameras, CCTVs, and baby monitors by unidentified perpetrators in 2016. Nicole Perlroth, "Hackers Used New Weapons to Disrupt Major Websites Across U.S.," *The New York Times*, October 21, 2016, https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.

72
KPMG, "Cybercrime Survey Report 2015," *KPMG*, November 30, 2015, https://home.kpmg.com/in/en/home/insights/2015/11/cyber-crime-survey-2015.html.

73
Indian Ministry of Electronics and Information Technology, "Draft IoT Policy Document," *Indian Ministry of Electronics and Information Technology*, accessed June 14, 2017, http://meity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf.

74
Dixit Sandeep, "Testing of Telecom Equipment in India Mandatory From Next Year," *The Hindu*, last modified July 13, 2016, http://www.thehindu.com/news/national/testing-of-telecom-equipment-in-india-mandatory-from-next-year/article6304138.ece.

75
"India Allows Telecoms Equipment Imports But Imposes Security Guidelines," *India Infoline News Service*, October 19, 2017, http://www.indiainfoline.com/article/news-top-story/india-allows-telecoms-equipment-imports-but-imposes-security-guidelines-113101401730_1.html.

76
This is a fictional scenario; the decision to use Yamaha was made on the basis of the company's drone development, as well as data available about the company. The scenario by no means intends to blame any particular company.

77
Yamaha, “Agricultural Use,” *Yamaha RMAX,* accessed June 14, 2017, https://www.yamahamotorsports.com/motorsports/pages/precision-agriculture-rmax.

78
Yamaha, “Yamaha Remotely Piloted Helicopters”, *Yamaha Motor Corporation*, accessed June 14, 2017, https://www.yamahamotorsports.com/motorsports/pages/precision-agriculture; Evan Ackerman, “Yamaha Demos Agricultural RoboCopter, But Humans Can’t Unleash It Yet,” *IEEE Spectrum*, October 16, 2014, http://spectrum.ieee.org/automaton/robotics/drones/yamaha-demos-agricultural-robocopter.

79
Kana Inagaki, “Yamaha Aims to Unlock US and EU Markets with Agricultural Drone,” *Financial Times*, July 5, 2015, https://www.ft.com/content/626684e2-2181-11e5-aa5a-398b2169cf79.

80
Quinten Plummer, “FAA Approves Yamaha RMAX Drone To Spray Crops In U.S.,” *Tech Times*, May 6, 2015, http://www.techtimes.com/articles/51049/20150506/faa-approves-yamaha-rmax-drone-to-spray-crops-in-u-s.htm.

81
Jie Ma and Yuki Hagiwara, “Will Drones Become the Toast of Napa?,” *Bloomberg*, February 18, 2016, http://www.bloomberg.com/news/articles/2016-02-18/in-napa-crop-dusting-drones-are-ready-for-takeoff.

82
Maps of India, “Top 10 Cotton Producing States of India,” *Maps of India*, accessed October 17, 2017, http://www.mapsofindia.com/top-ten/india-crops/cotton.html.

83
Environmental Justice Foundation, “The Deadly Chemicals in Cotton,” Pesticide Action Network White Paper, 2007, https://ejfoundation.org/reports/the-deadly-chemicals-in-cotton.

84
Mario Ballano Barcena and Candid Wueest, “Insecurity in the Internet of Things,” Symantec White Paper, 2015, https://www.symantec.com/content/en/us/enterprise/iot/b-insecurity-in-the-internet-of-things_21349619.pdf.

85
Scott Charney and Eric Werner, “Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency & Trust,” Microsoft White Paper, July 25, 2011, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REXXtT.

86
There is a tremendous amount written on supply chain risk management by a range of companies and U.S. governmental organizations. From the U.S. government standpoint, the National Institute for Standards and Technology (NIST) is a good place to start for detailed discussions on the issue. See NIST, “Cyber Supply Chain Risk Management,” NIST.gov, accessed August 17, 2017, http://csrc.nist.gov/scrm/. See also the archive of The Comprehensive National Cybersecurity Initiative (CNCI) of the Obama White House, “The Comprehensive National Cybersecurity Initiative,” obamawhitehouse.archives.gov, accessed August 17, 2017, https://obamawhitehouse.archives.gov/node/233086.

87
World Bank, “Agriculture, Value Added (% of GDP), The World Bank,” *World Bank,* accessed June 14, 2017, http://data.worldbank.org/indicator/NV.AGR.TOTL.ZS.

88
Id.

89
Id.

90
Michael Chui, James Manyika, and Mehdi Miremadi, "Where Machines Could Replace Humans—and Where They Can't (Yet)," *McKinsey Quarterly* (July 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet.

91
See Ford Motor Company, "How Connectivity Is Driving the Future of the Car," *Wired,* February 2016, https://www.wired.com/brandlab/2016/02/how-connectivity-is-driving-the-future-of-the-car/; see also Jim Resnick, "The Future of Mobility," *Wired*, December 2015, https://www.wired.com/brandlab/2015/12/the-future-of-mobility/. In the summer of 2017, Ford had a range of cybersecurity job positions advertised to support its investments in cybersecurity, which was reported by the local paper, the *Dearborn Press and Guide*, as a "top five" priority for Ford's research and development. Andrea Blum, "Ford, U of Michigan Create New Summer Internship Program," *Dearborn Press and Guide*, August 2, 2017, http://www.pressandguide.com/news/ford-u-of-m-dearborn-create-new-summer-internship-program/article_5376aa67-8e9f-59e8-8e48-86d541ae4c77.html. For jobs listings, see Ford's webpage, accessed August 17, 2017, http://corporate.ford.com/ListJobs/All/Search/jobtitle/cybersecurity/. For background on the vulnerability of driverless cars, see Nicole Perlroth, "Electronic Setups of Driverless Cars Vulnerable to Hackers," *New York Times*, June 7, 2017, https://www.nytimes.com/2017/06/07/technology/electronic-setups-of-driverless-cars-vulnerable-to-hackers.html?mcubz=1.

92
Reserve Bank of India, "Customer Protection–Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," *Reserve Bank of India*, accessed June 14, 2017, https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=3235.

93
In 2016, the debit cards of nearly 3.2 million Indian and foreign customers were compromised through vulnerabilities in the ATM transaction processing system designed by Hitachi Ltd. In this case, it was unclear how Hitachi was legally responsible as the point of entry for the fraud. Pratik Bhakta, "Hitachi Owns Up: Systems Compromised in 2016 Leading to Scare," *Economic Times*, accessed June 14, 2017, http://economictimes.indiatimes.com/articleshow/57058658.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

94
This recommendation mirrors prior public-private partnership initiatives between the U.S. government and the private sector in the United States. The detection of BlackEnergy malware in Ukraine helped spur the U.S. government in 2014–2015 to reach out to industrial control system (ICS) owners and operators across the country to plan for potential disruptions. See Industrial Control Security-Computer Emergency Response Team (ICS-CERT), "Alert (ICS-ALERT-14-281-01E): Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," *ics-cert.us-cert.gov,* last modified December 9, 2016, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

95
There are numerous American examples of such staffing structures. For public-private organizations, the U.S. government initiated the Enduring Security Framework, a public-private organization within the United States that brings together national security leaders with key companies in the information technology sector and critical infrastructure sector to discuss cybersecurity challenges. U.S. Department of Homeland Security, "Enduring Security Framework," *U.S. Department of Homeland Security*, https://www.dhs.gov/keywords/enduring-security-framework. Within the Department of Homeland Security, the Industrial Control Security-Computer Emergency Response Team briefs critical infrastructure owners and operators across the United States on cybersecurity risks that may affect them. See ICS-CERT, *supra* note 94. Within Microsoft, several cybersecurity groups exist whose purpose is to educate the public and engage governments to mitigate cyberrisks.

96
Ralph Jennings, "China-Vietnam Relations Fall To A One-Year Low Over A New Maritime Dispute," *Forbes,* July 31, 2017, https://www.forbes.com/sites/ralphjennings/2017/07/31/china-vietnam-relations-fall-to-a-one-year-low-over-a-new-maritime-dispute/#336df63a521a. See also Reuters, "Vietnam calls for Southeast Asian unity amid South China Sea tension," *Reuters*, August 23, 2017, https://www.reuters.com/article/us-southchinasea-vietnam-idUSKCN1B4099.

97
Companies like Tencent, Baidu, and Alibaba brought goods and services directly into the hands of average citizens; WeChat, the Chinese version of WhatsApp, has enabled the Chinese to book train tickets, pay their servants and electric bills, and express themselves through text and image-sharing social media. "WeChat for Web," *WeChat.com*, accessed November 12, 2017, https://web.wechat.com/.

98
Patrick Tucker, "Thanks, America! How China's Newest Software Could Predict, Track, and Crush Dissent," *DefenseOne*, March 7, 2016, http://www.defenseone.com/technology/2016/03/thanks-america-china-aims-tech-dissent/126491/.

99
For a look at consultative democracy in China, see, *inter alia,* Baogang He and Stig Thøgersen, "Giving the People a Voice? Experiments with Consultative Authoritarian Institutions in China," *Journal of Contemporary China* 19 (2010): 66; and Rose Yu, "A Scene From China's Experiment in 'Consultative Democracy,'" *Wall Street Journal*, March 9, 2015, http://blogs.wsj.com/chinarealtime/2015/03/09/a-scene-from-chinas-experiment-in-consultative-democracy/.

100
The CCP has allowed for a degree of "consultative democracy" that brought citizens and organizations and ethnic groups into conversation with the central government and provided avenues for airing political and social grievances; it also sought citizens' views on issues of corruption and environmental degradation. Yet freedom of assembly remains banned on the mainland; the Great Firewall prevents online organizing; and the jailing of journalists, human rights lawyers, and dissidents at home and, in some cases, extradition from overseas, continues. Two notable cases were the 2015 forcible extradition of asylum-seeking journalist Jiang Yefei and refugee publisher Dong Guangping from Thailand. See Reporters Without Borders, "China Pursues Journalists And Dissents Overseas," *Reporters Without Borders,* November 20, 2015, last modified January 20, 2016, https://rsf.org/en/news/china-pursues-journalists-and-dissidents-overseas.

101
See U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016," (Washington, D.C.: The Office of the Secretary of Defense, 2016), 64, http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf.

102
Mark Magnier, "China Data Augur More Weakness," *Wall Street Journal,* January 18, 2016, http://www.wsj.com/articles/china-data-augur-more-weakness-1453139758.

103
For more on China's middle class, see the *Economist*'s special report on Chinese society. In particular, see Rosie Blau, "The New Class War," *The Economist,* July 9, 2016, http://www.economist.com/news/special-report/21701653-chinas-middle-class-larger-richer-and-more-vocal-ever-threatens.

104
See PCA Case number 2013-19, *supra* note 2.

105
Ankit Panda, "1 Year Later: Reflections on China's Oil Rig 'Sovereignty Making' in the South China Sea," *The Diplomat,* May 12, 2015, http://thediplomat.com/2015/05/1-year-later-reflections-on-chinas-oil-rig-sovereignty-making-in-the-south-china-sea/.

106
Shannon Tiezzi, "Vietnam to China: Move Your Oil Rig Out of the South China Sea," *The Diplomat,* April 9, 2016, http://thediplomat.com/2016/04/vietnam-to-china-move-your-oil-rig-out-of-the-south-china-sea.

107
Associated Press, "Flight Info Screens at Vietnam's Two Major Airports Hacked," *Voice of America*, July 29, 2016, https://www.voanews.com/a/flight-info-screens-at-vietnam-major-airports-hacked/3441118.html.

108
Barack H. Obama, "Executive Order–Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," *White House*, April 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

109
This investigation is completely fictitious. For background on the actual Westinghouse indictments, however, see the U.S. District Court for the Western District of Pennsylvania's indictment of members of the People's Liberation Army: U.S. v. Wang, Sun, Wen, Huang, and Gu, No. 14-118 (W. D. PA May 1, 2014), accessed January 15, 2016, https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

110
Blake Hounshell, "Charter 08," *Foreign Policy,* October 8, 2010, http://foreignpolicy.com/2010/10/08/charter-08/. The document was translated by the Hong Kong-based NGO Human Rights in China, and was first published in "China Rights Forum," the organization's quarterly journal.

111
This behavior draws from an interview with a leading circumvention tool service provider. Per that interview, the magic number of users in a country to enable a mass increase in usage during an incident is reportedly ten thousand. With the initial number of 10,000 users, one circumvention tool quickly ramped up to 500,000 users in a short period of time in Iraq during an election period.

112
For views on Xi's relationship with the PLA and the PLA's political evolution, see Charles Clover, "Xi's China: Command and Control," *Financial Times,* July 26, 2016, https://www.ft.com/content/ddeoaf68-4db2-11e6-88c5-db83e98a590a.

113
See the mission statement of the People's Armed Police Force: Ministry of National Defense, People's Republic of China, "The People's Armed Police Force," *eng.mod.gov.cn,* accessed September 13, 2016, http://eng.mod.gov.cn/ArmedForces/armed.htm. See also Michael Wines, "China Approves Law Governing Armed Police Force," *New York Times,* August 27, 2009, http://www.nytimes.com/2009/08/28/world/asia/28china.html?_r=0.

114
For background on Xi's military reforms, see James Mulvenon, "China's "'Goldwater-Nichols'? The Long-Awaited PLA Reorganization Has Finally Arrived," *China Leadership Monitor* 49 (Winter 2016), http://www.hoover.org/sites/default/files/research/docs/clm49jm.pdf. See also Loro Horta, "PacNet #85—Understanding PLA Reforms," *Center for Strategic and International Studies,* December 15, 2015, https://www.csis.org/analysis/pacnet-85-understanding-pla-reforms.

115
A moderate increase in freedom of expression and democratization could be anticipated on the basis of recent economic indicators, as Larry Diamond argues. China now approaches previous democratizing states' GDP growth rates, nearing the per capita income that South Korea held at the time of its own democratic transition in 1987–88. Even with a slowdown, some analysts have argued that by 2020 China could reach the per capita income that Hungary and Mexico achieved during their democratic transitions. Larry Diamond, "The Coming Wave," *The Journal of Democracy* 23, no. 1 (2012): 5–13.

116
Id.

117
See David Sanger, “U.S. and China Seek Arms Deal for Cyberspace,” *New York Times,* September 19, 2015, http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?smid=tw-share&_r=0. See also John Kerry, “An Open and Secure Internet: We Must Have Both” (speech, Korea University, Seoul, South Korea, May 15, 2015), accessed September 12, 2016, https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm.

118
United Nations, General Assembly, *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (July 22, 2015), accessed September 18, 2016, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

119
See G7 Foreign Ministers at Lucca, *supra* note 32.

120
For a list of the thirteen root name servers, see Internet Assigned Names Authority, “Root Servers,” *Internet Assigned Names Authority,* accessed September 13, 2016, https://www.iana.org/domains/root/servers.

121
Echoing previous statements by U.S. Cyber Command leadership, the statement could include a line that both countries seek for their cybertools to be “louder” and identifiable – not only for purposes of demonstration and deterrence, but also to foster transparency within the international system. See reporting on statements by U.S. Cyber Command leadership, Chris Bing, “U.S. Cyber Command Director: We Want ‘Loud,’ Offensive Cyber Tools,” *FedScoop*, August 30, 2016, http://fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016.

122
For sources outlining the preconditions that can trigger political resistance to illegitimate and oppressive regimes, see Mohammed Hafez, *Why Muslims Rebel: Repression and Resistance in the Islamic World* (Boulder: Lynne Reiner Publishers, 2004).

123
Freedom House, “Freedom on the Net 2016,” *Freedom House*, accessed July 10, 2017, https://freedomhouse.org/report/freedom-net/freedom-net-2016.

124
See Philip N. Howard and Muzammil M. Hussain, *Democracy’s Fourth Wave?: Digital Media and the Arab Spring* (Oxford: Oxford University Press, 2013), 23.

125
For background on the Hong Kong pro-democracy protests of 2014, see Heather Timmons and Lily Kuo, “Did Hong Kong’s Pro-Democracy Protests Really Change Anything?” *Quartz,* December 12, 2014, https://qz.com/310479/did-hong-kongs-pro-democracy-protests-really-change-anything/. See also Quartz’s broader coverage on the 20th anniversary of the political handover of Hong Kong to China, “The Future of Hong Kong,” *Quartz,* accessed July 10, 2017, https://qz.com/on/the-future-of-hong-kong/.

126
Anonymous reportedly threatened China with online retaliations during pro-democracy protests in Hong Kong in 2014. See Douglas Ernst, “Anonymous Threatens China with Massive Cyberattack: ‘Operation Hong Kong’,” *Washington*

Times, October 10, 2014, http://www.washingtontimes.com/news/2014/oct/10/anonymous-threatens-china-with-massive-cyberattack/.

127
For benefits of the rule of law in preventing violence, counter-insurgency strategy, and the risks posed by governmental illegitimacy, see *inter alia* Ramachandra Guha, "Democracy and Violence, in India and Beyond," *Institute for Public Policy Research*, August 8, 2015, https://www.ippr.org/juncture/democracy-and-violence-in-india-and-beyond; and Rachel Kleinfeld and Harry Bader, *Extreme Violence and the Rule of Law: Lessons from Eastern Afghanistan* (Washington, D.C.: Carnegie Endowment for International Peace, 2014), 5, http://carnegieendowment.org/files/violence_rule_of_law.pdf. For a broader treatment of counterinsurgency tactics and issues of legitimacy, see also Alistair Horne, *A Savage War of Peace: Algeria 1954–1962* (New York: New York Review Books Classics, 2011) and David Kilcullen, *Counterinsurgency* (Oxford: Oxford University Press, 2011).

128
Outside of initiating or continuing a previously initiated armed struggle, however, a non-state group would be unlikely to purposely conduct an intentionally destructive cyberspace operation that would cause a loss of life, as it would likely initiate a forceful response by the state.

129
From 2014, the U.S. Department of Homeland Security has led a cross-sector, national effort to assess and analyze the cybersecurity risks associated with the United States' most important infrastructure. The Office of Cyber and Infrastructure Analysis oversees the effort, and as of October 2017 is directed in the United States by Brandon Wales. For the policy decisions that led to the creation of this office, see Exec. Order. No. 13636, 78 Fed. Reg. 11737 (February 19, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. For more on the Office of Cyber and Infrastructure Analysis, see U.S. Department of Homeland Security, "Office of Cyber and Infrastructure Analysis (OCIA)," *U.S. Department of Homeland Security,* last modified July 14, 2017, https://www.dhs.gov/office-cyber-infrastructure-analysis.

130
Ernst & Young, *Global Telecommunications Study: Navigating the Road to 2020* (London: EYGM, 2015), http://www.ey.com/Publication/vwLUAssets/ey-global-telecommunications-study-navigating-the-road-to-2020/$FILE/ey-global-telecommunications-study-navigating-the-road-to-2020.pdf.

131
The Economist, "What is China's Belt and Road Initiative?," *The Economist,* May 15, 2017, https://www.economist.com/blogs/economist-explains/2017/05/economist-explains-11.

132
Luke Grub and Sally Murphy, "Singapore's First Data Breach?," *Global Privacy & Security Compliance Law Blog*, August 21, 2014, http://www.globalprivacyblog.com/privacy/singapores-first-data-breach.

133
James Lu, "Security Firm Shows Xiaomi Smartphones Secretly Stealing Your Data (Updated)," *HardwareZone Singapore*, August 11, 2014, http://www.hardwarezone.com.sg/tech-news-security-firm-shows-xiaomi-smartphones-secretly-stealing-your-data-updated.

134
Matt Apuzzo and Michael S. Schmidt, "Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say," *New York Times*, November 15, 2016, https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html.

135
Eva Dou, “Chinese Tech Firm Tells Users: We May Hand Over Your Data to the Government,” *Wall Street Journal*, March 18, 2016, https://blogs.wsj.com/chinarealtime/2016/03/18/chinese-tech-firm-tells-users-we-may-hand-over-your-data-to-the-government/.

136
Bloomberg, “Chinese Draft Cyber Law Requires Security Assessment For Companies Exporting Data,” *South China Morning Post*, April 11, 2017, http://www.scmp.com/news/china/policies-politics/article/2086735/chinese-draft-cyber-law-requires-security-assessment.

137
Press Trust of India, “Xiaomi Shifts Phone User Data Out Of China On Privacy Concerns,” *The Hindu,* May 23, 2016, http://www.thehindu.com/business/Industry/xiaomi-shifts-user-data-out-of-china/article6530672.ece.

138
The term was first used by India’s foreign secretary Subrahmanyam Jaishankar to refer to Chinese investment along the Belt and Road Initiative determining market rules. See generally Ministry of External Affairs, Government of India, “Speech by Foreign Secretary at Raisina Dialogue in New Delhi” (speech, New Delhi, India, March 2, 2015), accessed June 14, 2017, http://mea.gov.in/Speeches-Statements.htm?dtl/26433/Speech_by_Foreign_Secretary_at_Raisina_Dialogue_in_New_Delhi_March_2_2015.

139
See Joel Snyder, “The Huawei Security Risk: Factors to Consider Before Buying Chinese IT,” *TechTarget* 1, no. 1 (2013), accessed July 6, 2017, http://searchsecurity.techtarget.com/feature/The-Huawei-security-risk-Factors-to-consider-before-buying-Chinese-IT.

140
National Development and Reform Commission (NDRC), People’s Republic of China, “Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road,” *NDRC, People’s Republic of China*, last modified March 28, 2015, http://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html.

141
Asian Infrastructure Investment Bank, “Articles of Agreement,” *Asian Infrastructure Investment Bank*, accessed June 14, 2017, https://www.aiib.org/en/about-aiib/basic-documents/_download/articles-of-agreement/basic_document_english-bank_articles_of_agreement.pdf.

142
Lorraine Luk, “China’s Top Telecom Carriers to Sell Tower Assets to Joint Venture,” *Wall Street Journal*, October 15, 2015, http://www.wsj.com/articles/chinas-top-telecom-carriers-to-sell-tower-assets-to-joint-venture-1444886966.

143
AidData, “ZTE builds Pacifctel’s $50M Fibre Optic Line,” *AidData*, accessed September 20, 2016, http://china.aiddata.org/projects/35724. See also ZTE, “ZTE Optical Fiber Transmission System for Pacifictel in Ecudor,” ZTE, last modified December 12, 2003, http://wwwen.zte.com.cn/endata/magazine/ztetechnologies/2002year/no5/articles/200312/t20031212_161169.html.

144
International Telecommunications Union (ITU), “Cyberwellness Profile Cambodia,” *ITU*, August 26, 2014, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Cambodia.pdf; ITU, “Cyberwellness Profile Lao People’s Democratic Republic,” *ITU,* August 12, 2014, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Lao_PDR.pdf; ITU, “Cyberwellness Profile Republic Of Tajikistan,” *ITU*, March 9, 2015, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Tajikistan.pdf; ITU, “Cyberwellness Profile Kyrgyz Republic”, *ITU*, March 10, 2015, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Kyrgyzstan.pdf.

145
Tajikistan and Kyrgyzstan currently provide arterial routes for China's Silk Road Economic Belt, the land component of the Belt and Road Initiative. Laos and Cambodia are in talks with China to link their highways with the 21st-century Maritime Silk Road, which forms the maritime "Road" of the Belt and Road Initiative. The Chinese government is currently re-thinking its original plan to designate the Vietnamese port city of Hai Phong as a major sea-link in the Belt and Road Initiative. This follows the 2016 International Tribunal on the Law of the Sea (ITLOS)'s award on the South China Sea dispute between China and the Philippines. The ruling negated Beijing's "historical claims" to the Sea. The failure of all parties to arrive at a satisfactory Declaration of Conduct in the South China Sea consequently deteriorated relations between China and Vietnam. China is now eager to court and influence political and business constituencies in Cambodia and Laos, with a view toward replacing Vietnam as a key link in the Belt and Road Initiative. See Hong Kong Trade and Development Council (HKTDC), "What is Belt and Road Initiative," *HKTDC.com,* accessed June 14, 2017, http://beltandroad.hktdc.com/en/about-the-belt-and-road-initiative/about-the-belt-and-road-initiative.aspx.

146
See *supra* note 145.

147
For background on China's approach to data security and encryption, see Yuan Yuang, "China's Cyber Security Law Rattles Multinationals," *Financial Times,* May 30, 2017, https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996. See also KPMG China, "Overview of China's Cybersecurity Law," KPMG Advisory, 2017, https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

148
See *supra* note 141 at Article 13.

149
Sanjay Vijayakumar, "Facebook Seeks India Payment System Patent," *The Hindu*, June 4, 2017, http://www.thehindu.com/business/facebook-seeks-india-payment-system-patent/article18714301.ece.

150
Ministry of Foreign Affairs, People's Republic of China, "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," *Ministry of Foreign Affairs, People's Republic of China*, last modified March 28, 2015, http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1249618.shtml.

151
U.S. Department of the Treasury, "The Committee on Foreign Investment in the United States (CFIUS)," *U.S. Department of the Treasury*, last modified December 20, 2012, https://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx.

152
The United States Department of Homeland Security has already conducted this analysis and may be able to help advise Asian countries on best practices.

153
Andy Greenberg, "How An Entire Nation Became Russia's Test Lab For Cyberwar," *Wired,* June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

154
Nathaniel Persily, "Can Democracy Survive the Internet?," *Journal of Democracy* 28, no. 2 (2017): 63-75, http://www.journalofdemocracy.org/sites/default/files/07_28.2_Persily%20%28web%29.pdf. In the article, Persily makes a persuasive argument for how fake news, data manipulation, and online populist rhetoric altered the 2016 U.S. presidential election. Persily also recognizes that the 2016 U.S. election may have been a one-off event that was created by a unique confluence

of economic and political forces. He writes, “Democracy depends on both the ability and the will of voters to base their political judgments on facts, or at least on strong intermediary institutions that can act as guardrails to channel decision making within the broad range of democratic alternatives. The premium placed on virality of messages, the threat to accountability posed by unrestrained anonymity, and the undercutting of sovereignty presented by an open Internet pose novel challenges for democracy in the United States. The election of Donald Trump may, indeed, be a ‘one-off,’ as it is difficult to think of many people with his particular personality qualities, strengths, and motivations. Nonetheless, the playbook for one type of successful candidacy and campaign in the Internet age has now been demonstrated. Whether others can succeed with the same playbook remains to be seen.” *Id.* at 72.

After conducting a brief review of the status of efforts by social media companies and other technology companies to undercut the risks Persily raises, he points out that technology solutions may not be able to solve the problems inherent in American democracy at the moment, saying, “With the deterioration in democratic values occurring both on- and offline, we should not expect technology to rescue us from the historical and sociological forces currently threatening democracy, even if that same technology facilitated the disruption in democratic governance in the first instance.” *Id.* at 75. The solution to the current rise in ethnic nationalism and populism in the United States and other countries may lie in part with technology, but the greater effort may rest with good political leadership, in building inclusive political values that protect the well-being of the whole, in extending a just rule of law, and in growing civic and democratic engagement. This ultimately has more to do with developing effective leadership, and with growing legitimate, inclusive political parties, than with technology.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley