CYBER COMPETITION IN THE INDO-PACIFIC GRAY ZONE 2035

ARMY CYBER INSTITUTE
AT WEST POINT

GDIL

TEXAS
The University of Texas at Austin

WEST POINT
PRESS

Disclaimer: The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Military Academy, United States Army, United States Department of Defense, or United States Government.

This report is supported by U.S. Army Grant #W911NF-23-2-0098.

CYBER COMPETITION IN THE INDO-PACIFIC GRAY ZONE 2035

A technical report by
Kevin J. Lentz*, Jason C. Brown,
Kylie J. Heitzenrater, Akemi Hosoya,
Joe Eduard Rucker, Kelli Sutton-Bosley

ARMY CYBER INSTITUTE AT WEST POINT

GDIL

TEXAS
The University of Texas at Austin

*Corresponding authors: kevinjameslentz@utexas.edu

THREATCASTING PARTICIPANTS

Victoria Chevallier

Jewells Escamilla

Jonathan Rose, U.S. Department of State

Alexander Tiberghien, The Citadel

Ambrose Kam, Lockheed Martin

Kylie J Heitzenrater, The University of Texas at Austin

Gary Williams, Lockheed Martin

Albert Zhang, Australian Strategic Policy Institute

Kelli Sutton-Bosley, Norwich University

Robert Andrew Ward, University of North Georgia

Kevin Lentz, The University of Texas at Austin

Miles Zoellner

Franki Harah E. Alano

Anonymous

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report is the result of collaborative research between the Global Disinformation Lab at The University of Texas at Austin and the Army Cyber Institute at West Point. In October 2023, a cross-functional group of practitioners convened in Austin, Texas to answer the following primary research question: How should the U.S. and Indo-Pacific allies and partners organize and coordinate their defensive cyber efforts to prevail in the next decade of competition with China? Utilizing the Threatcasting method of inquiry, these practitioners developed twenty-five scenarios on the topic by simulating people in places experiencing threats that could emerge in the next decade. A team of analysts then analyzed these scenarios and incorporated additional relevant research on the region to produce indicators of how these threats might emerge. This report discusses major findings, indicators, trends, and recommendations for practitioners to put into action to disrupt, mitigate, or recover from the threats.

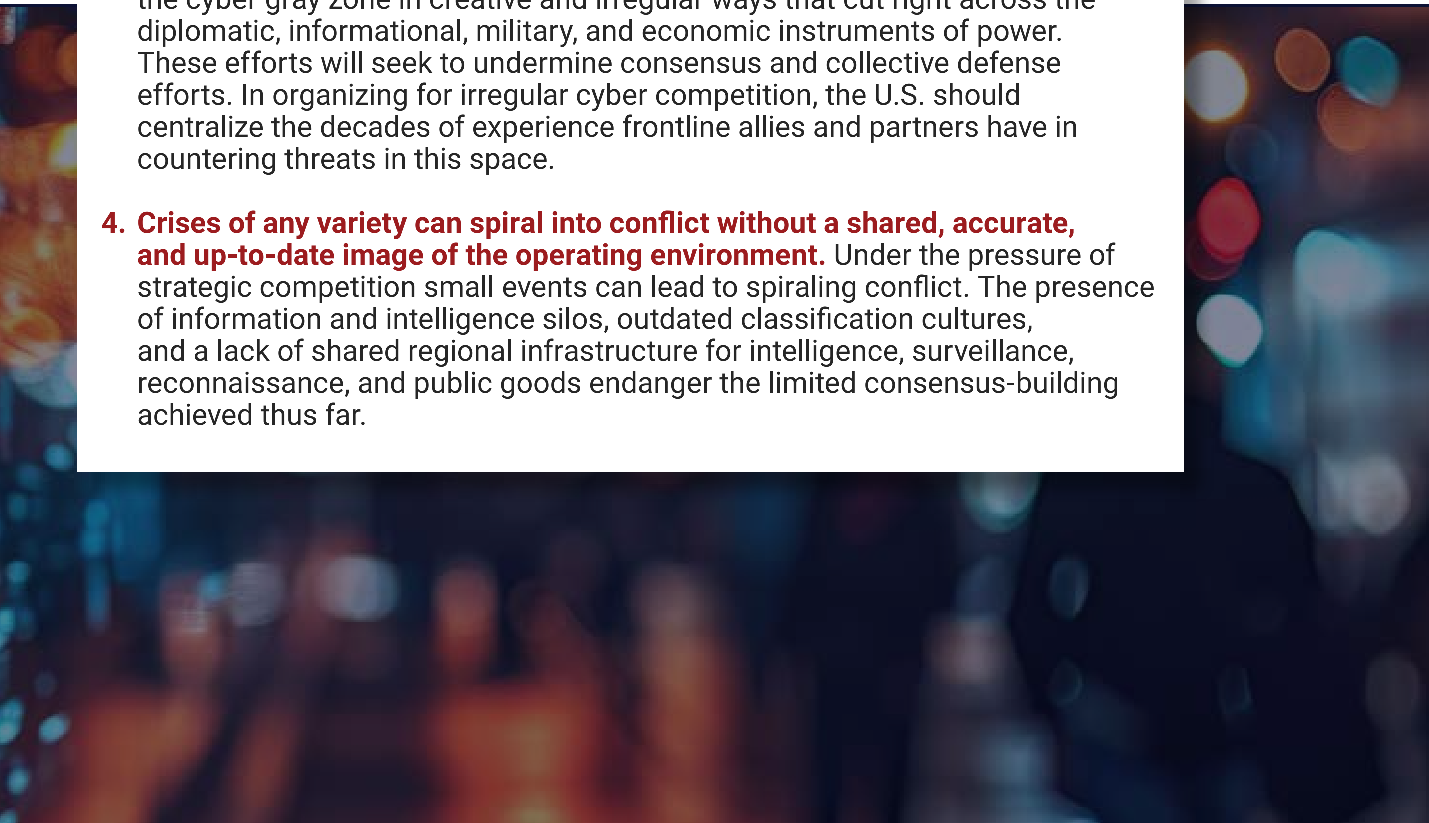
FINDINGS

1. **Third-party cyber kingmakers will make or break efforts to organize cyber-inclusive treaties and defense coalitions.** These cyber kingmakers consist of two groups: multinational tech companies with nation-state level cyber capabilities and the multi-aligned states of the Indo-Pacific. South and Southeast Asian states are poised to remain multi-aligned while reaping benefits from both great power contenders. Tech companies, on the other hand, are limited in their geopolitical engagement by market logic. Successful cooperative cyber defense will depend on mobilizing the interests of these kingmakers.

2. **Fragmented regulatory authority will continue to compound regulatory lag.** Cyber-adjacent regulators are producing a labyrinth in their attempt to fill regulatory vacuums. Moreover, the question of which agencies regulate and engage in 'cyber' activities—and their methods of doing so—is being addressed diversely across Indo-Pacific countries. This variance undermines consensus on gray zone practices, the organization of military cyber defense, and norms surrounding emerging technologies. Interoperability will remain a mirage if policies don't interlock and cyber organizations don't have clear counterparts.

3. **The irregular strategic competition between the U.S. and the Chinese Communist Party will set the parameters for the use and development of cyber power.** Deterred conventionally, the CCP will continue to exploit the cyber gray zone in creative and irregular ways that cut right across the diplomatic, informational, military, and economic instruments of power. These efforts will seek to undermine consensus and collective defense efforts. In organizing for irregular cyber competition, the U.S. should centralize the decades of experience frontline allies and partners have in countering threats in this space.

4. **Crises of any variety can spiral into conflict without a shared, accurate, and up-to-date image of the operating environment.** Under the pressure of strategic competition small events can lead to spiraling conflict. The presence of information and intelligence silos, outdated classification cultures, and a lack of shared regional infrastructure for intelligence, surveillance, reconnaissance, and public goods endanger the limited consensus-building achieved thus far.



RECOMMENDATIONS

Meeting the threats of the 2035 Indo-Pacific cyber gray zone requires holistic thinking and a sense of urgency. These three overarching recommendations are the most critical. Further recommendations are provided at the end of each findings section and at the end of the report.

1. **The U.S. should develop and operationalize a distinct cyber economic trade and development strategy for the region.** Cyberspace is a warfighting domain housed overwhelmingly in private infrastructure. The question of which nation's tech companies build out cyber infrastructure in the Indo-Pacific, and under which rules, will determine the key terrain of the Indo-Pacific cyberspace in which the U.S. and its allies will compete. Losing cyber market share to the CCP will doom the U.S. and allies and partners to a permanent uphill battle in cyberspace. Without coordinated government assistance, the cyber development efforts of aligned tech kingmakers will likely be economically uncompetitive, unfocused, and strategically ineffective. Further, efforts to tack cyber on to much larger trade frameworks, like the Indo Pacific Economic Framework, subject this time-sensitive need to slow and frequently derailed political processes.

2. **The U.S. should rebuild and re-center political and information warfare capabilities for cyber competition.** Forging consensus and building collective cybersecurity in the Indo-pacific will require years of concerted messaging from across government silos. Moreover, cyber has emerged as the primary vector for the information operations necessary to enhance and monitor the efficacy of this messaging. The U.S. further needs the capacity to conduct information operations successfully in contested and expeditionary spaces that have received little attention historically. Achieving this goal demands cultural sensitivity, rapidity, adaptability, and scalability—qualities lacking in our current government approach, which is fragmented and assigns low priority to political and information warfare.

3. **The U.S. should work with allies and partners to develop an Indo-Pacific cyber and conventional open-access intelligence clearinghouse.** Opaque motives, crises, and overreactions will characterize the next decade of the Indo-pacific gray zone. Without a clear and shared operational understanding of the conventional and informational environment, de-escalation will be unacceptably dependent on chance and good fortune. Current intelligence clearinghouses range from military-specific classified mission partner environments at one end to public-private data fusion centers at the other, with a thicket of media and academic efforts in between.[1] The U.S. should take the lead in integrating government and private intelligence pipelines into a reliable open-access portal for allies and partners that provides reliable information and intelligence on cyber and conventional domains.

[1] "Allies, Partners Tap into Technology to Monitor Maritime Domain." Indo-Pacific Defense Forum, November 14, 2023. https://ipdefenseforum.com/2023/11/allies-partners-tap-into-technology-to-monitor-maritime-domain/.

INTRODUCTION

“The problem of finding a way to block Communist expansion in the Gray Areas is one of the most perplexing of U.S. foreign policy.”[2]

[2] Thomas K. Finletter, Power and Policy: U.S. Foreign Policy and Military Power in the Hydrogen Age, 1st ed. (New York: Harcourt, Brace, 1954), 129.

So wrote former Secretary of the Air Force Thomas Finletter, assessing the geopolitical situation in 1954.[3] Comparing the Indo-Pacific with Europe, Finletter attributed the stability of the latter to three pillars: (1) the consensus (to defend against Soviet expansion), (2) the treaty (NATO), and (3) the defense forces (the European and American militaries). In contrast, in the Indo-Pacific, all three pillars were lacking. There was little consensus among Indo-Pacific countries that the regional threat (communist China) was actually a threat, only a handful of bilateral off-shore security alliances existed, and there was no unified command of a regional defense force.

Approaching the problem again nearly a century later using the Threatcasting method, our cross-functional group of practitioners found many of the same political obstacles as Finletter did in his time. The key differences between then and now only emerge from the interplay of this familiar problem set with the novel and dynamic technological environment of our present and near future.

Keeping the broader strategic competition in mind, this project aimed to answer two questions:

(1) How should the U.S. and Indo-Pacific allies and partners organize and coordinate their defensive cyber efforts to prevail in the next decade of competition with China?

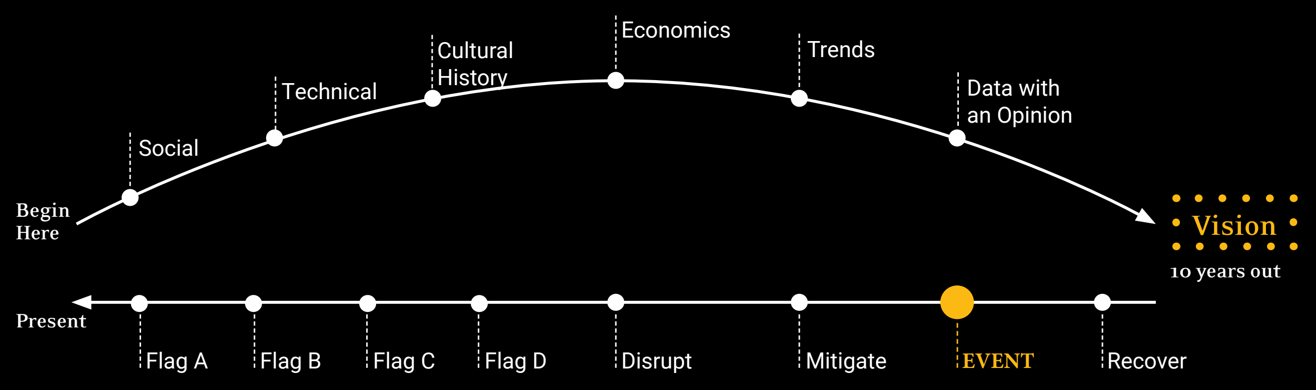
(2) What are the current and anticipated legal and policy bottlenecks hindering more effective standalone and combined cyber defensive efforts in the region?

[3] Unlike today when the term 'gray zone' evokes functional images of Chinese coast guard boats and cyber attacks, in 1954 'gray areas' referred to a geographical image. It was the politically non-aligned rim of the Eurasian continent spanning from Iraq to Taiwan. See Appendix C.

THREATCASTING

Threatcasting is a methodology used to help multidisciplinary groups envision future scenarios. It is also a process that enables systematic planning against threats for up to ten years in the future. Utilizing the Threatcasting methodology,[4] groups explore possible future threats and how to transform the future they desire into reality while mitigating a set of threats. Threatcasting is a continuous, multi-step process with comprehensive inputs. These inputs encompass a range of disciplines, including social science, technical research, cultural history, economics, trends analysis, expert interviews, and science fiction storytelling, informing the exploration of potential visions of the future.

Image 1. The Threatcasting Methodology, adapted from Johnson, B. D., Vanatta, N., & Coon, C. (2021). Threatcasting. Morgan and Claypool.



[4] B. D. Johnson, N. Vanatta, and C. Coon, *Threatcasting* (San Rafael, CA: Morgan & Claypool, 2021).

The outcome is the beginning of a set of possible threats, evolving indicators, and recommended actions that, if taken, can mitigate challenges to undesired futures. These projected outcomes are not definitive, but they give organizations a starting point.

Participants synthesized the data into guided workbooks by drawing research inputs from a wide variety of subject matter expert interviews and then conducted three rounds of Threatcasting sessions.

These Threatcasting sessions acted as simulations, generating numerous scenarios, each depicting a person in a place experiencing a threat. Following the workshop, analysts methodically analyzed these scenarios to categorize and aggregate novel indicators, assessing how the most plausible threats could manifest in the next decade and identifying potential implications for "gatekeepers" mitigating these threats.

The output of the methodology provides organizations and decision-makers with a framework to plan, prepare, and make decisions in a complex and uncertain environment. Threatcasting guards against strategic surprise. When a crisis occurs or an opportunity presents itself, a decision-maker or a leader is better prepared. With this, their response is more likely to be, "We have talked about this before. We know where to start..."

FINDINGS AND RECOMMENDATIONS

FINDING #1: THIRD PARTY CYBER KINGMAKERS

In 15th century England two houses competed for the English throne. Unable to ascend or remain in power of their own means, a powerful third party, the Duke of Warwick, held sway over royal governments during a generation of civil war. His outsized impact on the fate of English monarchs led people to call him "Warwick the Kingmaker".

English history doesn't directly concern us, but the idea of powerful party 'kingmakers' does. When established powers cannot overcome one another through their own means, previously marginal actors in key structural positions emerge as de-facto sovereigns. In the context of gray zone competition in cyberspace, our models consistently encountered two groups of kingmakers who preside over the competition between the U.S. and China: political-economic kingmakers, such as multi-aligned Indo-Pacific nation states, and technological kingmakers, such as Google.

Political-economic

The nation-states of South and Southeast Asia are among the largest growth engines of the global economy. This is especially so regarding the digital economy, with some of the youngest, fastest growing, internet-hungry economies in the world.[5] The politicians brokering access to these markets play a key role in determining the legal and technical rules of their own cyberspaces, as well as the economic well-being of the companies and countries that construct those cyberspaces. These nation-state-level decisions in turn will impact their capacity—and that of their chosen partners—to perceive, respond, and shape the Indo-Pacific cyberspace.

Laos, for example, has engaged Huawei to build out their telecommunications infrastructure as part of the new China-Laos 'Smart Highway' and railway system which will run through the entire country. Given that Chinese firms will operate and maintain the cyber-integrated rail and highway, Laos is effectively locked into the CCP technological ecosystem for decades.[6] The resulting political-economic impact is clear and measurable. Reasonable minds can infer that Laos will feel pressured to look to Beijing on debates about cybersecurity norms—at a minimum—for the foreseeable future. Moreover, CCP-directed companies now have a decades-long market, data source, and captive political customer in Laos. It is easy to foresee the CCP leveraging this political momentum to propel further cyber megaprojects in the region.

As illustrated by the Laos example, South and Southeast Asian states are central to the future global digital economy. An Indonesia choosing U.S. or partnered companies as digital development partners, or an India drifting from the Quad to hammer out a cooperative development plan with China unilaterally will have a greater impact on the Indo-Pacific cyberspace than the combined actions of the U.S., allied, and partnered cyber practitioners. The U.S. and its allies and partners will have to win the trust of these political-economic kingmakers, bearing in mind that they each have their own national interests.[7]

[5] "Posts Tagged Southeastern Asia." *DataReportal – Global Digital Insights*, February 23, 2024. https://datareportal.com/reports. See also "Digital ASEAN." World Economic Forum. Accessed March 31, 2024. https://www.weforum.org/projects/digital-asean/; S. Chiang, "Southeast Asia's Digital Economy May Be Set to Hit $1 Trillion, but Roadblocks Remain," *CNBC*, June 1, 2023. https://www.cnbc.com/2023/06/01/aseans-digital-economy-has-great-potential-but-roadblocks-remain.html; and "Asia Poised to Drive Global Economic Growth, Boosted by China's Reopening." *IMF*, May 1, 2023. https://www.imf.org/en/Blogs/Articles/2023/05/01/asia-poised-to-drive-global-economic-growth-boosted-by-chinas-reopening.

[6] D. Mochinaga, "The Digital Silk Road and China's Technology Influence in Southeast Asia." *Council on Foreign Relations.* Accessed March 31, 2024; https://www.cfr.org/blog/digital-silk-road-and-chinas-technology-influence-southeast-asia.

[7] "Digital Economy Framework Agreement (DEFA): ASEAN to Leap Forward Its Digital Economy and Unlock US$2 Tn by 2030." *ASEAN Main Portal,* August 19, 2023. https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/.

Technological

The second category of kingmakers is the constellation of powerful tech companies that dominate global cyberspace. As a uniquely privatized domain, the multinational internet service providers, cloud service providers, small but disruptive artificial intelligence innovators, and critical supply chain vendors that own and operate global cyberspace are its de-facto sovereigns. For example, while Russian cyber forces face off with Ukrainian counterparts as state adversaries, they do so on Amazon, Microsoft, and Google servers.[8][9][10] Another case in point is the new joint U.S.-Australian undersea internet cable to the Pacific Islands. These nation-states are not going to build and operate it—Google is.[11] A third testament to the outsized influence of these cyber giants is the appointment of formal ambassadors by numerous nation-states to represent their interests to tech companies.[12] As Denmark's tech ambassador phrased it: "What has the biggest impact on daily society? A country in southern Europe, or in Southeast Asia, or Latin America, or would it be the big technology platforms?"[13]

"What has the biggest impact on daily society? A country in southern Europe, or in Southeast Asia, or Latin America, or would it be the big technology platforms?"

-Casper Klynge,
Danish Ambassador to
Technology Industry

[8] B. Smith, "Defending Ukraine: Early Lessons from the Cyber War," *Microsoft on the Issues*, June 22, 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[9] B. Nolan, "Zelenskyy Awards Amazon the Ukraine Peace Prize After AWS Helped Save Its 'Digital Infrastructure,'" *Business Insider*. Accessed March 31, 2024. https://www.businessinsider.com/zelenskyy-amazon-ukraine-peace-prize-digital-war-support-aws-2022-7.

[10] F. Konkel, "Ukraine Tech Chief: Cloud Migration 'Saved Ukrainian Government and Economy,'" *Nextgov.com*, December 1, 2022. https://www.nextgov.com/digital-government/2022/12/ukraine-tech-chief-cloud-migration-saved-ukrainian-government-and-economy/380328/.

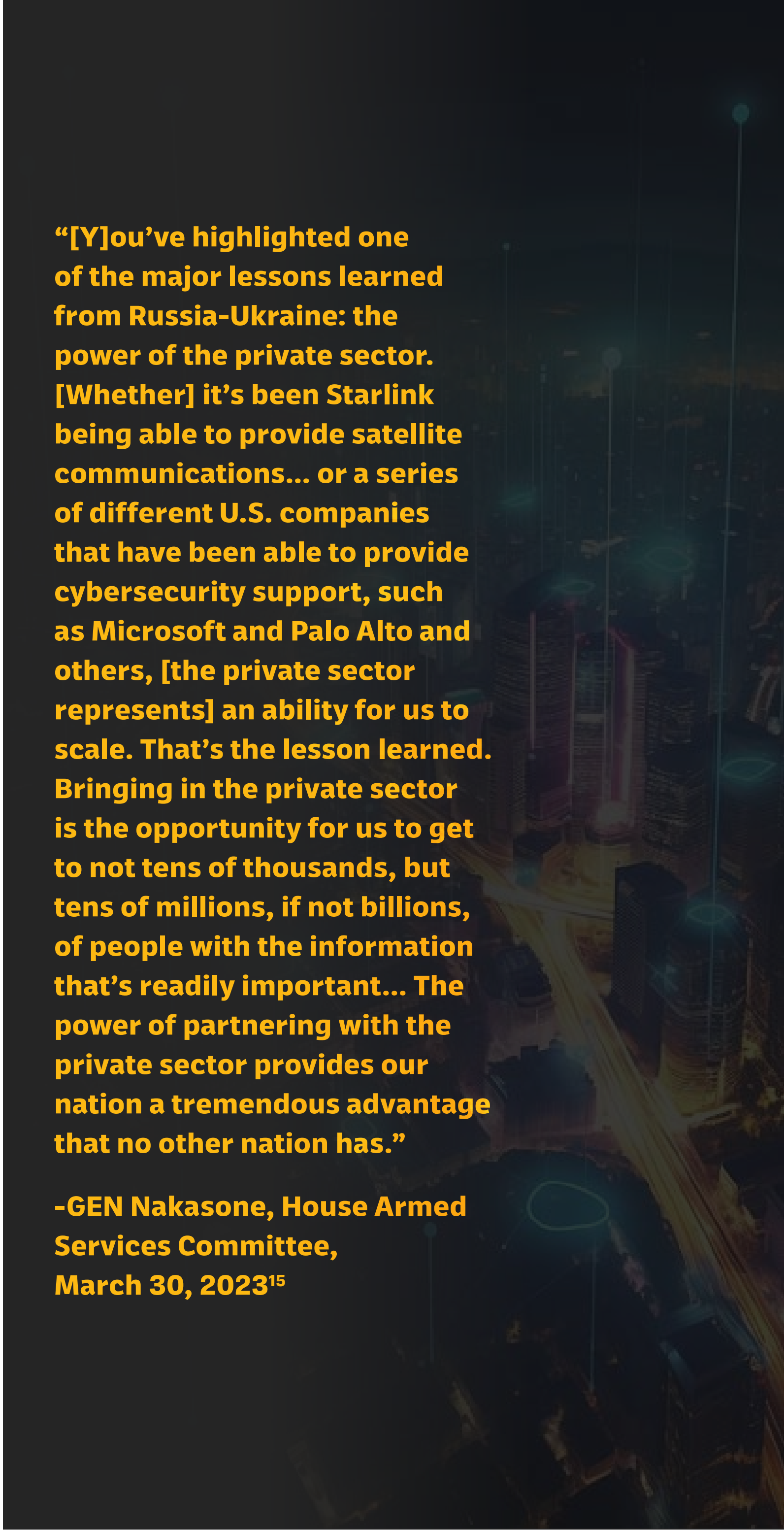
[11] T. Hunnicutt, "Exclusive: Google to Run Internet Cables to Pacific Islands in Australia-U.S. Deal," *Reuters*, October 25, 2023. https://www.reuters.com/technology/google-run-internet-cables-pacific-islands-australia-us-deal-2023-10-25/.

[12] L. Clarke, "Tech Ambassadors: Redefining Diplomacy for the Digital Era," *Tech Monitor*, February 16, 2021. https://techmonitor.ai/leadership/innovation/tech-ambassadors.

[13] As quoted in, A. Satariano, "The World's First Ambassador to the *Tech Industry*," *The New York Times,* September 3, 2019. https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html. In accordance with this sentiment, the United Kingdom, Austria, a dozen other states, and eventually the European Union have all established diplomatic outposts in Silicon Valley. See S. Stolton, "The European Union Opens a Silicon Valley 'Embassy,'" *POLITICO,* March 29, 2024. https://www.politico.com/newsletters/digital-future-daily/2022/08/09/the-european-union-opens-a-silicon-valley-embassy-00050576.

However, technological kingmakers are also subject to disruption. Relatively unknown but nimble innovators can quickly shift the private sector balance of power. OpenAI, for instance, is a prime example of a global disruptor. As late as October 2022, OpenAI was only known to industry insiders as one of many artificial intelligence companies Microsoft had made a large investment in. By April 2023, its CEO was having a private meeting with the Prime Minister of Japan.[14]

In cyberspace, nation-states can only effectively intervene through a private sector tech partner, often in ways that devolve sovereign functions from the modern nation-state to these companies. Outside of miniscule government enclaves (.mil, .gov), sprawling private companies run the current internet in massive virtual versions of twentieth century company towns, complete with cyber police departments, firefighters, legal and policy teams, and the complete suite of administrative functions. How U.S. cyber defenders can leverage the resources of these private kingmakers in a planned, sustained, effective, and mutually beneficial way is a central question for the next decade:



"[Y]ou've highlighted one of the major lessons learned from Russia-Ukraine: the power of the private sector. [Whether] it's been Starlink being able to provide satellite communications... or a series of different U.S. companies that have been able to provide cybersecurity support, such as Microsoft and Palo Alto and others, [the private sector represents] an ability for us to scale. That's the lesson learned. Bringing in the private sector is the opportunity for us to get to not tens of thousands, but tens of millions, if not billions, of people with the information that's readily important... The power of partnering with the private sector provides our nation a tremendous advantage that no other nation has."

-GEN Nakasone, House Armed Services Committee, March 30, 2023[15]

[14] A. Oikawa, K. Takeuchi, and M. Ban, "OpenAI CEO Vows to Work with Japan on User Protections," *Nikkei Asia*. Retrieved March 31, 2024. https://asia.nikkei.com/Business/Technology/OpenAI-CEO-vows-to-work-with-Japan-on-user-protections.

[15] Congress.gov, "Cyberspace Operations: Conflict in the 21st Century," March 30, 2023. Retrieved March 31, 2024. https://www.congress.gov/event/118th-congress/house-event/115618.

Box 1 - U.S. Tech Companies and the War in Ukraine[16]

Microsoft has been a pivotal ally to Ukraine since Russia's full-scale invasion. In addition to protecting Ukraine's critical digital infrastructure from cyberattacks, Microsoft has also provided $100 million dollars' worth of free support and services for their digital products to ensure that Ukrainian government agencies, digital infrastructures, and civilian lives can run smoothly through Microsoft's cloud. Alongside technological expertise and aid, the company has also supported humanitarian organizations efforts in Ukraine and provided data and support to international organizations documenting Russian war crimes. Eight months after the start of the war, Microsoft had provided over $400 million dollars of aid and support to Ukraine.[17]

SpaceX has also provided integral internet services across Ukraine to schools, hospitals, and municipal governments, in addition to helping drones strike Russian targets through their Starlink network. In conjunction with monetary support from USAID, SpaceX has kept Ukrainians connected to the internet despite destruction of cell transmission towers.[18][19]

[16] See José Ignacio Torreblanca, "Ukraine One Year On: When Tech Companies Go to War," *ECFR,* March 7, 2023. https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/.

[17] Brad Smith, "Extending Our Vital Technology Support for Ukraine," *Microsoft On the Issues,* November 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

[18] Alex W. Salkever, "How Elon Musk's Starlink Got Battle-Tested in Ukraine," *Foreign Policy*, April 2, 2024, https://foreignpolicy.com/2022/05/04/starlink-ukraine-elon-musk-satellite-internet-broadband-drones/.

[19] Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," *Carnegie Endowment for International Peace,* accessed March 31, 2024, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

Recommendations

1. **The U.S. should develop and operationalize a distinct cyber economic trade and development strategy for the region.** Cyberspace is a warfighting domain housed overwhelmingly in private infrastructure. The question of which companies build out cyber infrastructure in the Indo-Pacific, and under whose rules, will determine the key terrain of the Indo-Pacific cyberspace in which the U.S. will compete. Losing cyber market share to the CCP will doom the U.S. and allies and partners to a permanent uphill battle in cyberspace. Without coordinated government assistance, the cyber development efforts of aligned tech kingmakers will likely be economically uncompetitive, unfocused, and strategically ineffective. Moreover, attempts to integrate cyber into larger trade frameworks hold hostage the urgent need to address slow and frequently derailed political processes.

2. **The U.S. should incentivize joint research and development with allies and partners on key cyber technology areas.** Joint research and development offers a strong option for the U.S. and its allies and partners to generate kingmaker buy-in to U.S. priorities. It also enables the generation of policy and technical interoperability at a very early stage of nascent technological development. Key areas to prioritize include general purpose artificial intelligence, autonomous weapons and surveillance systems, next generation encryption, and analog countermeasures to cyber-degraded command and control.

3. **The U.S. and capable allies and partners should incentivize cybersecurity and information security training courses for public officials.** The targeting of public officials frequently recurred in our threat models. Public officials are high value targets for cyber espionage and subversion for two reasons: (1) their proximity to the levers of power, and (2) a pervasive absence of dedicated training on next generation threats. The level of training varies across the region but may be higher in areas where older generation politicians are overseeing rapid technological development in their country. A network is only as strong as its weakest node. As receivers of sensitive information and intelligence, public officials must heighten their awareness of and training for cyber and information threats.

FINDING #2: COMPOUNDED REGULATORY LAG

Our threat models frequently displayed a known pattern. Technological innovations leap ahead of regulatory regimes opening up legal and operational gray areas which adversaries then take advantage of. However, our models displayed a further twist: the attempt of existing regulators to close down these gray zones results in ad-hoc and unhelpful innovations in the regulatory structures themselves. The result is new or newly ordained, overlapping, and contradictory regulators annexing power in these gray areas which sets off bureaucratic turf wars and slows progress while the rapid pace of innovation continues to widen the legal and operational gray area. As a result, actors experiencing threats in this space are confronted with unclear defenders, confusing authority structures, limited assistance, and a general lack of standardized response procedures.

Cybersecurity incident reporting regulation in the U.S. is a good example of this dynamic. Each year the U.S. economy is subjected to a bewildering number of costly cyberspace losses from ransomware and other cyber-enabled forms of fraud, extortion, and intellectual property theft. The exact scope and cost of this annual raiding is unknown, as there exists no overarching federal cyber incident reporting law that compels the victims of these attacks to report them. Instead, an overlapping patchwork of federal and state regulators, from the U.S. Securities and Exchange Commission (SEC) to the Department of Health, to each individual state have worked up a tangle of over two dozen reporting regulations (not counting state requirements) covering a hodge-podge of industries. Each of these reporting rules, moreover, have different thresholds for disclosure, reporting timelines, mobilizing authorities, and scopes.[20][21]

Recognizing the cost this ad-hoc system imposes on private industry and national security, the government authorized the Cybersecurity and Infrastructure Security Agency (CISA) in 2022 to develop and implement reporting regulations for covered entities, which would effectively act as a centralized federal reporting law.[22] However, progress is slow. The process of implementing this law began with a call for information and extensive industry consultations in September 2022 which then resulted in a notice of proposed rulemaking on

[20] Melanie Brooks and Steven Lesmes, "Cybersecurity Incident and Breach Reporting Requirements," *R Street Institute,* accessed March 31, 2024, https://www.rstreet.org/commentary/cybersecurity-incident-and-breach-reporting-requirements/.

[21] Ibid.

[22] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," accessed March 31, 2024, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia. https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/

March 27th, 2024.[23] After an initial two months for public comment, another 16 months (to September 2025) are allotted before publication of the final rule. Naturally, the actual implementation of these new authorities will itself be a difficult learning process for an agency less than a decade old.

Meanwhile, other regulators in this space, like the Securities and Exchange Commission, continue to unilaterally expand their reach and create further complications while technology companies persist, naturally, in pushing the next generation of disruptive products and applications to market.[24] This tenuous situation—young organizations gaining new power and turfing with more established regulators—can easily happen in the defense space, where lawmakers today debate the need to stand up a dedicated cyber service branch.[25]

[23] Federal Register, "Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022," September 12, 2022, https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022. See also Brandon Wales, "CIRCIA at One Year: A Look Behind the Scenes," *CISA*, March 24, 2023, https://www.cisa.gov/news-events/news/circia-one-year-look-behind-scenes.

[24] Catalin Vasquez, "SEC Disclosure Rule for 'Material' Cybersecurity Incidents Goes into Effect," *CyberScoop*, December 18, 2023, https://cyberscoop.com/sec-cybersecurity-incidents-disclosure-rule/.

[25] Serbu, J. (n.d.). *Does the military need a separate service for cyber? Some lawmakers think so; DoD isn't sure.* Retrieved March 31, 2024, from https://federalnewsnetwork.com/defense-news/2023/04/does-the-military-need-a-separate-service-for-cyber-some-lawmakers-think-so-dod-isnt-sure/.

Box 2 - Back to the Drawing Board: European AI Delayed After OpenAI

The difficulty of regulating emerging technology can be seen in the creation of the European Union's AI Act. The act was first introduced to the European commission on April 21, 2021, and sought to broadly cover single-use cases of artificial intelligence technology through a risk-based approach.[26] For example, the use of AI in the medical sector would be deemed high risk due to potential negative consequences on human life and would have to abide by stricter rules and regulations.

While the initial draft provided a workable foundation, the rapid rise of ChatGPT forced lawmakers to rethink and rework the AI Act to include regulations and compliance on general purpose AI systems, foundation models, and generative AI. Ultimately, the updated AI Act was finally passed on December 9, 2023, after two years of deliberation, and is set to be enforced in stages, with full enforcement of the Act starting in 2026.[27]

The creation of the EU's AI Act raises a few concerns for regulating emerging technologies. The first is the amount of time it takes from creation to enforcement of regulation—a five-year window. Particularly when compared to the speed with which tech products and advancements hit consumer markets, this lag risks diminishing the effectiveness of any policies. The second is the futureproofing and longevity of such regulations. During the creation of the AI Act, major additions had to be made to accommodate the rapidly developing AI landscape. Only time will tell if what policymakers envisioned in 2023 will still hold in 2026 when the Act is fully enforced. Another major cause of concern is that the AI Act will enforce substantial monetary compliance costs for companies. This poses the risk of hindering innovation and creating monopoly behavior in the market—investors and entrepreneurs may stray away from AI tech startups due to the increased capital costs that they will incur from the regulated market.[28] This will give immense leverage to larger companies who can afford these costs.[29]

[26] Hainsdorf, C., Hickman, T., Lorenz, S., & Rennie, J. (2023, December 14). *Dawn of the EU's AI Act: Political agreement reached on world's first comprehensive horizontal AI regulation | White & Case LLP.* https://www.whitecase.com/insight-alert/dawn-eus-ai-act-political-agreement-reached-worlds-first-comprehensive-horizontal-ai

[27] Prohibited AI Systems will be enforced 6-months after the act's finalization; provisions on general purpose AI systems will be enforced 12-months after; and all other provisions will be enforced in 2026.

[28] In a report by the Center for Data Innovation, it was estimated that the additional cost for compliance for a high-risk AI system can reach up to €400,000. Benjamin Mueller, "AI Act Would Cost the EU Economy €31 Billion Over 5 Years, and Reduce AI Investments by Almost 20 Percent, New Report Finds," *Center for Data Innovation*, July 26, 2021, https://datainnovation.org/2021/07/ai-act-would-cost-the-eu-economy-e31-billion-over-5-years-and-reduce-ai-investments-by-almost-20-percent-new-report-finds/.

[29] These larger companies are likely to be those already established in the U.S. Relatedly, the Federal Trade Commission has launched an investigation into generative AI investments and partnerships looking at Microsoft and OpenAI, Amazon and Anthropic, and Google and Anthropic. See “FTC Launches Inquiry into Generative AI Investments and Partnerships,” *Federal Trade Commission*, January 24, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships.

STORY 1:
HOW TO LOSE MALAYSIA

LTC Thompson wondered to himself as he walked from the rack to his duty station onboard the USS Longhorn. Everything had been going surprisingly well. The PLA Navy coast guard ships had stopped harassing them during FONOPS, The Belt and Road seemed dead in the water from all the bad debt the CCP took on, and more impressively, the U.S., Japan, and Australia had started the roll-out of the flagship Blue Dot Network infrastructure projects across the Indo-Pacific. The CCP overall seemed to be willing to live with a lot less than they had originally wanted for themselves in the Indo-Pacific. Not bad.

“What the hell’s the matter with you?”

Schwartz, the E-5 due to deliver the 0500 briefing, watched Thompson silently with an ashen look. He didn’t respond.

“Well, we’re all here. Please proceed, sir.”

Schwartz glanced at his notes and began.

“From 0100 to 0330 one of the new automated stacker cranes installed by the Japanese at Port Klang malfunctioned tipping over dozens of containers and killing several Malaysian longshoremen. The software controls for the crane were non-responsive and the Japanese engineering team appears to have been off duty at a bar in Klang. Preliminary estimates put the dead at over a dozen, mostly Malaysians, but also at least one Japanese engineer, and the economic costs are in the millions and climbing. The Malaysian government has closed the port until the rest of the new port facilities can be safely brought back online. The Malaysian PM has summoned both the Japanese and American ambassadors.”

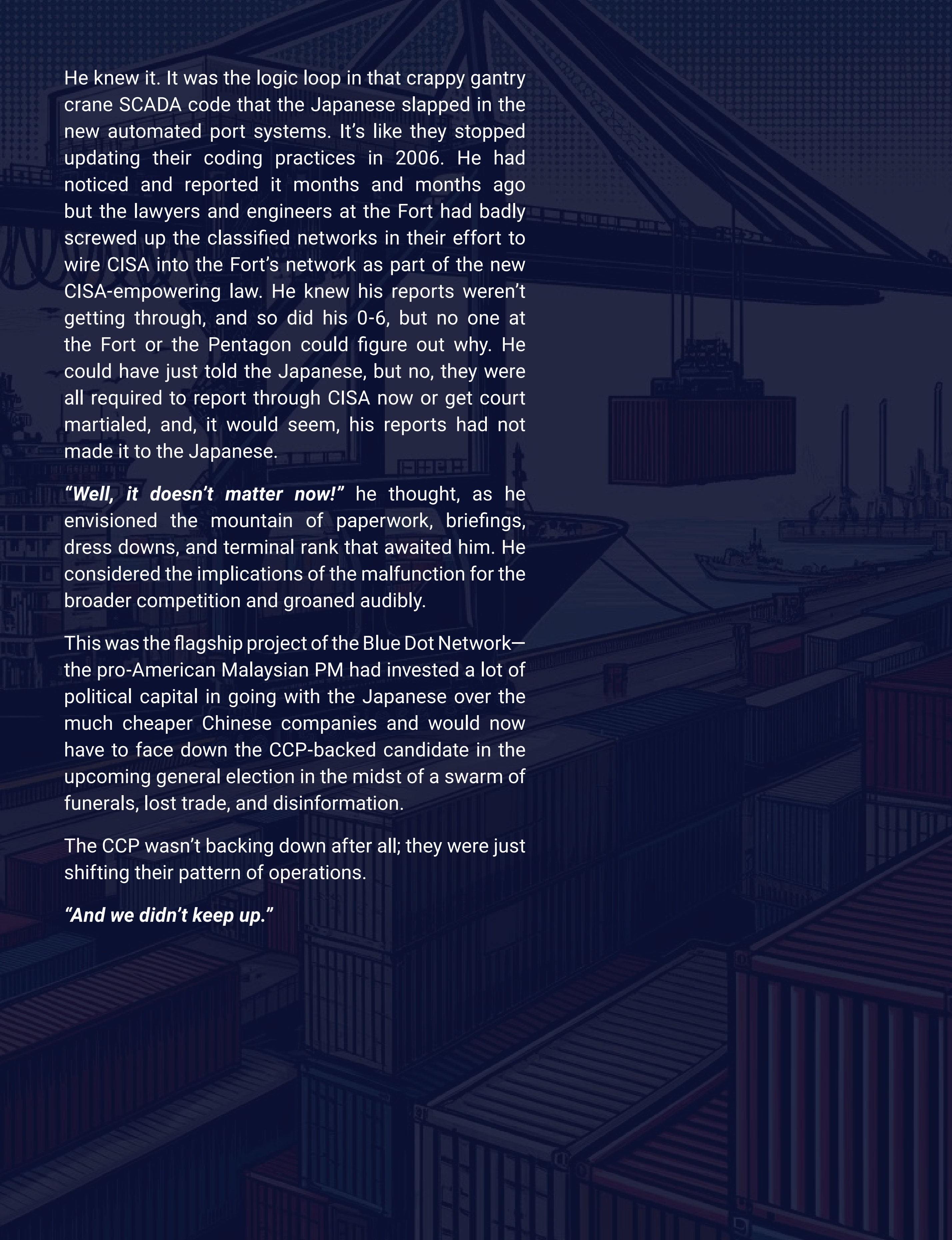
The room was silent. Thompson realized he was gripping his armrest tightly. His mind raced.

“What else?”

Schwartz shifted his weight to his other foot.

“There are several different conspiracy theories pinning the blame on the Blue Dot Network circulating through Tiktok and Facebook that preliminary intel from NSA traces back to digital MSS fronts.”

Thompson cursed himself in his mind. He felt cold sweat forming on the back of his neck.



He knew it. It was the logic loop in that crappy gantry crane SCADA code that the Japanese slapped in the new automated port systems. It's like they stopped updating their coding practices in 2006. He had noticed and reported it months and months ago but the lawyers and engineers at the Fort had badly screwed up the classified networks in their effort to wire CISA into the Fort's network as part of the new CISA-empowering law. He knew his reports weren't getting through, and so did his 0-6, but no one at the Fort or the Pentagon could figure out why. He could have just told the Japanese, but no, they were all required to report through CISA now or get court martialed, and, it would seem, his reports had not made it to the Japanese.

"Well, it doesn't matter now!" he thought, as he envisioned the mountain of paperwork, briefings, dress downs, and terminal rank that awaited him. He considered the implications of the malfunction for the broader competition and groaned audibly.

This was the flagship project of the Blue Dot Network—the pro-American Malaysian PM had invested a lot of political capital in going with the Japanese over the much cheaper Chinese companies and would now have to face down the CCP-backed candidate in the upcoming general election in the midst of a swarm of funerals, lost trade, and disinformation.

The CCP wasn't backing down after all; they were just shifting their pattern of operations.

"And we didn't keep up."

Recommendations

1. **The U.S. should more quickly centralize and streamline cyber regulatory power.** The confused status quo serves neither the economy nor national security. Reducing the noise in U.S. cyber regulation will clarify and accelerate a clearer situational awareness of cyber threats. This in turn will enable more effective information sharing within the U.S. government and among the ally and partner network. Though not a silver bullet, CISA is a clear focal point for this effort.

2. **The U.S. should share timely information on its cyber-regulatory development with Indo-Pacific allies and partners to cultivate interlocking policies and organizations.** Compounded regulatory lag frustrates the need to create interoperable policies and organizations for cyber defense. While respecting our political process, we can save time by dedicating resources to explaining developments and lessons learned to interested Indo-Pacific allies and partners who are also developing their cyber defense policies and organizations. Doing so will help prevent the independent evolution of non-interoperable policies and organizations in the Indo-Pacific ally and partner network.

FINDING #3: IRREGULAR COMPETITION IN CYBERSPACE

Across our models, Chinese Communist Party (CCP) cyber operations were overwhelmingly motivated by the political aim of separating Indo-Pacific allies and partners from the U.S.-led coalition and subordinating them to the will of Beijing. These cyber operations took the form of sabotaging and subverting diplomatic, informational, military, and economic targets through a wide variety of vectors. By leveraging cyber capabilities, these operations conducted forms of irregular warfare without the 'warfare.'[30]

Cyber defenders in this space will accordingly have to prepare for the long-term utilization of cyber operations that bypass conventional escalation norms. Furthermore, these irregular cyber operations support broader campaign objectives in the context of U.S.-Chinese political competition and cannot be separated from that context.

Importantly the success of this model of irregular competition is made possible by an Indo-Pacific cyberspace defined by three primary characteristics:

1. Vulnerable by design
2. Contested Cyber norms
3. Cyber defense resource gaps

Vulnerable by design

CISA, alongside a dozen domestic and international partners, define 'secure by design' as meaning, "technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure."[31]

Despite the efforts CISA and partners have made recently, our models describe a continuation of today's speed-over-security technological ecosystems: indigenous social media platforms poisoned by curated content pushed at scale, technical backdoors in shiny new server farms, sabotaged banking platforms, hacked navigation systems, and the like. In the coming decade the nascent effort of the U.S.-led coalition to secure cyberspace will struggle against the momentum of the historically open and insecure computer and internet technologies and protocols. In other words, the internet will remain 'vulnerable by design' due to the priority of economic over security incentives that mobilize production of current and future cyber technologies.

[30] J. C. Lumbaca, *Irregular Competition: Contemporary Lessons Learned and Implications for the Future* (2023), 3.

[31] "Shifting the Balance of Cybersecurity Risk: Security-by-Design and Default Principles," *CISA*, April 13, 2023, https://www.cisa.gov/news-events/alerts/2023/04/13/shifting-balance-cybersecurity-risk-security-design-and-default-principles p, 8.

Contested Cyber Norms

While the European Union's General Data Protection Regulation (GDPR) codifies shared regional norms for data security and privacy, the Indo-Pacific remains a fragmented and inconsistent norm landscape. Data security and cybercrime stand out as two particularly contested norms.

Regarding data security, many Indo-Pacific countries have expressed favor for data localization, which requires physical storage and safe transfer of data in certain places and ways, as opposed to free flow.[32] Some states consider this an avenue for development, as the effects of data localization could allow for government savings in data accessibility and competitive advantage for local industries.[33] Others warn of the possibility to alienate foreign investors by creating conflicting standards and forcing multiple restructurings of sectors that already feel burdened by regulatory compliance.

Cybercrime represents another contested norm. India, for example, stands out for corporatizing a proliferation of startups dedicated to corporate espionage, blackmail investigations, and other activities as designated by their clients in a broad 'hack-for-hire' industry. Companies like Appin Security Group, and its successor BellTroX, train employees under the guise of cybersecurity education and white hat hacking.[34] In reality, these firms are paid to hack the emails of high-profile individuals and obtain access to their networks and information. While the Indian government publicly disavows these activities, some researchers suggest the government may in fact sponsor them.[35]

Cyber Defense Resource gaps

The Indo-Pacific is an uneven mix of developed and developing economies marked by the historical contexts of colonialism, the Cold War, and now strategic competition. The systematic development of cyber power, meanwhile, is a nascent phenomenon in which even the most developed economies struggle to standardize manning, training, equipping, and doctrinal concepts across their legacy militaries.[36] As a result, the current Indo-Pacific landscape of cyber defense organizations is characterized by highly

[32] *The Asia Pacific Data Localisation Guide 2023*. Deloitte Taiwan. Accessed March 31, 2024. https://www2.deloitte.com/tw/en/pages/risk/articles/asia-pacific-data-localisation-guide-2023.html.

[33] Antoinette Sayeh, Era Dabla-Norris, and Tidiane Kinda, "Asia's Productivity Needs a Boost That Digitalization Can Provide," *IMF,* January 9, 2023. https://www.imf.org/en/Blogs/Articles/2023/01/09/asias-productivity-needs-a-boost-that-digitalization-can-provide.

[34] Raphael Satter and Christopher Bing, "How Mercenary Hackers Sway Litigation Battles," *Reuters,* June 30, 2022. https://www.reuters.com/investigates/special-report/usa-hackers-litigation/.

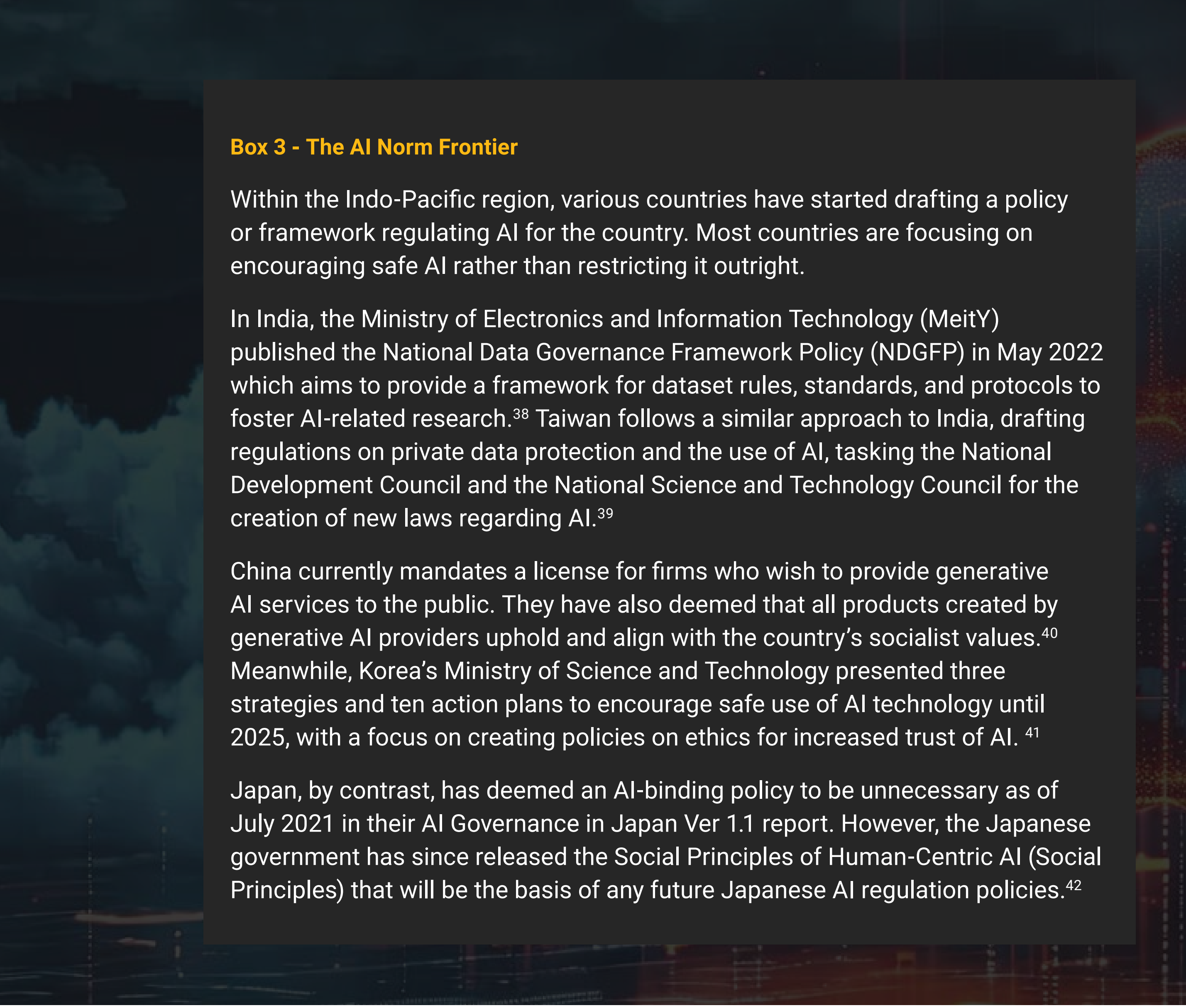
[35] Tom Hegel, "Elephant Hunting | Inside an Indian Hack-For-Hire Group—SentinelOne," accessed November 17, 2023. https://web.archive.org/web/20231117061038/https://www.sentinelone.com/labs/elephant-hunting-inside-an-indian-hack-for-hire-group/.

[36] Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford: Oxford University Press, 2022).

uneven levels of resourcing, different technical and doctrinal standards, and different political priorities.[37] In this context, different Indo-Pacific countries have different levels of ability to perceive, respond, and shape the regional cyberspace.

These respective cyber force structures and resourcing levels in turn affect the ability of American and allied and partnered actors to integrate their defensive cyber efforts.

[37] B. Hogeveen, "The Future of Cyber Warfare in the Indo-Pacific," Policy Commons, accessed May 24, 2024, https://policycommons.net/artifacts/3376700/the-future-of-cyber-warfare-in-the-indo-pacific/4175546/ . See also J. Blessing, "The Global Spread of Cyber Forces, 2000–2018," *13th International Conference on Cyber Conflict (CyCon)* (2021): 233–255, https://doi.org/10.23919/CyCon51939.2021.9467807.



Box 3 - The AI Norm Frontier

Within the Indo-Pacific region, various countries have started drafting a policy or framework regulating AI for the country. Most countries are focusing on encouraging safe AI rather than restricting it outright.

In India, the Ministry of Electronics and Information Technology (MeitY) published the National Data Governance Framework Policy (NDGFP) in May 2022 which aims to provide a framework for dataset rules, standards, and protocols to foster AI-related research.[38] Taiwan follows a similar approach to India, drafting regulations on private data protection and the use of AI, tasking the National Development Council and the National Science and Technology Council for the creation of new laws regarding AI.[39]

China currently mandates a license for firms who wish to provide generative AI services to the public. They have also deemed that all products created by generative AI providers uphold and align with the country's socialist values.[40] Meanwhile, Korea's Ministry of Science and Technology presented three strategies and ten action plans to encourage safe use of AI technology until 2025, with a focus on creating policies on ethics for increased trust of AI. [41]

Japan, by contrast, has deemed an AI-binding policy to be unnecessary as of July 2021 in their AI Governance in Japan Ver 1.1 report. However, the Japanese government has since released the Social Principles of Human-Centric AI (Social Principles) that will be the basis of any future Japanese AI regulation policies.[42]

[38] G. Hardias, S. Kim Sohee, and A. Brahmecha, "The Key Policy Frameworks Governing AI in India," Access Partnership, October 2, 2023, https://accesspartnership.com/the-key-policy-frameworks-governing-ai-in-india/.

[39] "Government drafting basic law to regulate AI," *Taipei Times*, July 6, 2023, https://www.taipeitimes.com/News/taiwan/archives/2023/07/06/2003802773.

[40] Forbes EQ BrandVoice, "How Does China's Approach to AI Regulation Differ from the U.S. and EU?," *Forbes*, accessed March 31, 2024, https://www.forbes.com/sites/forbeseq/2023/07/18/how-does-chinas-approach-to-ai-regulation-differ-from-the-us-and-eu/.

[41] Press Releases—과학기술정보통신부, accessed March 31, 2024, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=509&searchOpt=ALL&searchTxt=.

[42] H. Habuka, "Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency," *Center for Strategic & International Studies,* 2023, https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7-presidency.

Box 4 - Cyber Norms and the Digital Silk Road

In 2015, the Digital Silk Road Initiative (DSR) was formally announced as part of the China's Belt and Road Initiative (BRI) with the goal of increasing global digital connectivity, extending China's influence, and creating a China-centric regional digital infrastructure. While the PRC provides government aid and support to sponsoring nations, the DSR also incentivizes Chinese tech companies, such as Huawei, to further invest abroad.[43]

Developing nations in Eastern Europe, Latin America, Southeast Asia, the Middle East, and Africa represent a huge market for inexpensive, high-quality technology to expand internet connectivity and digital infrastructure. Currently, Chinese firms are filling this gap by providing technology and infrastructure, but also establishing training and development programs to foster technological cooperation in areas such as artificial intelligence, clean energy, and robotics.[44]

The DSR is an attempt by China and Chinese firms to spread the idea of 'cyber sovereignty' to developing countries, creating an alternate ideal of the internet where illiberal and authoritarian regimes are justified and can thrive.[45] This objective becomes clearer when examining the amount of surveillance and censorship technology that Chinese tech companies are exporting to authoritarian regimes. Huawei has created a network that connects thousands of surveillance cameras for the Kenyan police department, for example, while ZTE has provided the Ethiopian government access to surveillance technology that monitors internet and phone calls.[46]

[43] "Assessing China's Digital Silk Road Initiative," *Council on Foreign Relations,* accessed March 31, 2024, https://www.cfr.org/china-digital-silk-road.

[44] E. Masood, "How China is Redrawing the Map of World Science," *Nature,* May 1, 2019, https://www.nature.com/articles/d41586-019-01124-7.

[45] C. Dakota, "Community Watch: China's Vision for the Future of the Internet," *Atlantic Council,* December 4, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/community-watch-chinas-vision-for-the-future-of-the-internet/.

[46] R. Gallagher, "Export Laws: China is Selling Surveillance Technology to the Rest of the World." *Index on Censorship, 48(3), 35-37*. https://doi.org/10.1177/0306422019876445.

STORY 2:
THE CYBER DOPPELGANGER

"Is it good, are we on?"

"Yes, sir. Meeting is live." Jane gave a thumbs up from the corner of the office, just in front of the American flag.

"Ambassador Shimizu! Thank you for your call earlier today. You have my deepest apologies that I did not answer in a timely manner." A quick bend at the waist, difficult while seated, but manageable. ***"My superior needed me urgently. Now, to what do I owe the pleasure?"***

There was a brief pause while the translator hurriedly echoed Ambassador Patra's greeting. It had been nearly a month since the unexplained beginning of reduced communication between the two diplomats. His Japanese counterpart sat like a statue, displeasure and unease carved into his whole being. It was a sharp departure from his typical cheery disposition. Suddenly, the man rose from his chair and began what Nagasaki understood as beratement in any language. The translator spoke with furrowed brows.

"What is the meaning of this? Are you trying to pretend nothing happened? You can't ruin the single most important project of our careers and then lie to my face the very same day."

Patra tried to project calm bewilderment. A glance to the confused and panicked faces of his staffers offered neither comfort nor explanation. He held up his hands askance.

"Ambassador Shimizu, I'm afraid I don't know what you're talking about."

"You don't what I'm talking about?" he spat. ***"We were scheduled to finalize the joint cybersecurity initiative with the Minister of Foreign Affairs. You sat in that seat not six hours ago and disrespected the entire committee. My superiors will never let that policy see the floor of the Diet now. How could you let months of work burn to the ground and answer my call with a smile?"***

In his nearly twenty years of service, Ambassador Patra had endured many crisis situations. The trial by fire that new diplomats undergo in the State Department forged an unwavering and resourceful character in the man. Now, he felt like a fresh recruit, blood chilled by the genuine betrayal that showed in his counterpart's voice and body. He needed to fix this, quickly. How was he supposed to fix this? Start with the facts. Start with what you know.

"Ambassador Shimizu, I must insist that there is a misunderstanding. Our meeting with Minister Yamada is not for another month. We didn't have a call earlier today. I was in a meeting with the Deputy Secretary of State for Policy. Please help me understand what happened."

"I cannot accept this behavior. Inform my staff when you are prepared to acknowledge and apologize for this disgrace—and for when you have a plan for how we can go forward now, though I doubt there is a way."

The meeting box closed abruptly.

Patra stared back at his own pixelated puzzled face. The only sound in the office was the soft tap that came as he clicked open his emails in vain for some kind of explanation. Rapid footsteps approached the office door.

"Ambassador, you're going to want to hear this," the INR analyst in the doorway was breathless. Patra waved her in, and she began briefing immediately.

"Sir, we discovered a breach in the U.S.-JP diplomatic network environment. We don't know the full extent nor the scope of the breach. Initial assessments indicate that any of your communications within the past 35 days could have been meddled with. We also found dozens of .wav files and .jpegs from a root kit excavation that we believe may have been used to operate a deepfake. Sir, has Japan given any indication that they know?"

Everything quickly clicked into place in Patra's mind. The briefings, the inexplicable news reports, the increasing number of Chinese-language threats on his life, the disinformation mitigation policy with Japan, and now the baffling behavior of Ambassador Shimizu all swirled together in a dreadful haze.

The CCP had been middle-manning his relationship with Shimizu with a cyberized doppelganger.

The briefer waited for an answer with an arched eyebrow.

"No, I don't think they know."

Recommendations

1. **The U.S. should rebuild and re-center political and information warfare capabilities.** Building both consensus and collective cybersecurity in the Indo-pacific will require years of determined messaging from across government silos. Moreover, cyber has become the primary vector for the information operations needed to enhance and monitor the effectiveness of that messaging. The U.S. further needs the capacity to conduct information operations successfully in contested and expeditionary spaces that have received little attention historically. This will require cultural sensitivity, speed, flexibility, and scale that the currently de-prioritized and siloed approach to political and information warfare lacks across the U.S. government.

    - **In this effort, the U.S. should prioritize information campaigns designed to seize initiative in expeditionary spaces**. Priorities in this regard are belt and road recipient countries and historically under-prioritized developing economies in the Pacific Islands and Southeast Asia. Other recommendations in this report, especially those regarding Cyber Tradecraft, will hinge on the effectiveness of these expeditionary information efforts.

2. **The U.S. should centralize cybersecurity and information resilience training for frontline allies and partners.** Taiwan has decades of critical experience receiving and recovering from CCP irregular tactics in cyberspace. These tactics include espionage, subversion, and disinformation. Prevailing in irregular cyber competition requires that the U.S. understand and adopt lessons from the Taiwanese model while clarifying points where the threat from the CCP diverges in form. Australia also has a long history of CCP influence and cyber operations that the U.S. should proactively try to learn from, including countering legislation.

3. **The U.S. should work with allies and partners to develop an Indo-Pacific cyber and conventional open-access intelligence clearinghouse.** Opaque motives, crises, and overreactions will characterize the next decade of the Indo-Pacific gray zone. Without a clear and shared operational understanding of the conventional and informational environment, de-escalation will be unacceptably dependent on chance and good fortune. Current intelligence clearinghouses range from military-specific classified mission partner environments at one end to public-private data fusion centers at the other, with a thicket of media and academic efforts in between.[47] The U.S. should take the lead in integrating government and private intelligence pipelines into a reliable open-access portal for allies and partners that provides reliable information and intelligence on the cyber and conventional domains.

[47] "Allies, Partners Tap into Technology to Monitor Maritime Domain," *Indo-Pacific Defense Forum,* November 14, 2023, https://ipdefenseforum.com/2023/11/allies-partners-tap-into-technology-to-monitor-maritime-domain/.

FINDING #4: THE SHARING IMPERATIVE

The pressure of strategic competition has the potential to transform natural, political, and conventional and unconventional military crises into cascading miscalculations. While civil unrest, border skirmishes, and civil wars cause their own level of chaos, events like natural disasters, covert actions, or human error can occur with little to no warning and ripple across the region and globe. As globalization has increased the speed and effect radius of all crises, it is imperative to re-energize cyber-enabled information sharing agreements (ISAs) and public goods to mitigate the threat of regional crises spilling over into strategic miscalculation.

Importantly, norms for sharing crisis information exist. The Responsibility to Protect, or R2P, was adopted in 2005 by the United Nations and seeks to protect populations from mass atrocities, crimes against humanity, war crimes, and ethnic cleansing.[48] Expanding R2P to cover natural disasters has been considered but risks undermining the ability of the R2P to rally international support in response to events.[49] Nevertheless, natural disasters provide a category of unrest unique from other disasters as no nation is immune from the damaging effects. As the world's population continues to amass in urban areas linked to water routes for shipping, the consequences of a single natural disaster continue to grow. Within the Indo-Pacific region, there are nineteen megacities (defined as having an urban population greater than or equal to ten million citizens). The cities, along with the Indo-Pacific region in general, are highly vulnerable to natural disasters as the strong seasons, active tectonic plates, surrounding volcanoes, and dramatic topography create a "violent natural environment."[50]

In any case, while the norms and interests exist, the physical infrastructure to support them in the Indo-Pacific are either non-existent, underdeveloped, or under integrated. A recent example is the Quad group's Indo Pacific Maritime Domain Awareness (MDA) initiative.[51] By leveraging commercial satellite imagery and existing data fusion centers the MDA aspires to provide real time information

[48] "The Rise and Fall of the Responsibility to Protect," CFR Education from the Council on Foreign Relations, 2024, https://education.cfr.org/learn/timeline/rise-and-fall-responsibility-protect ; See also T. Dahl-Eriksen, "Responsibility to Protect and Rising Asian Powers," *Millennial Asia* 13, no. 2 (2022): 225–242, https://doi.org/10.1177/0976399621989464.

[49] G. Evans, "The Responsibility to Protect in Environmental Emergencies," *Crisis Group*, March 26, 2009, https://www.crisisgroup.org/global/responsibility-protect-environmental-emergencies.

[50] F. Gassert, S. Burke, and R. Zimmerman, "UPTEMPO: The United States and Natural Disasters in the Pacific," New America, 2019, https://www.newamerica.org/resource-security/reports/uptempo-united-states-and-natural-disasters/.

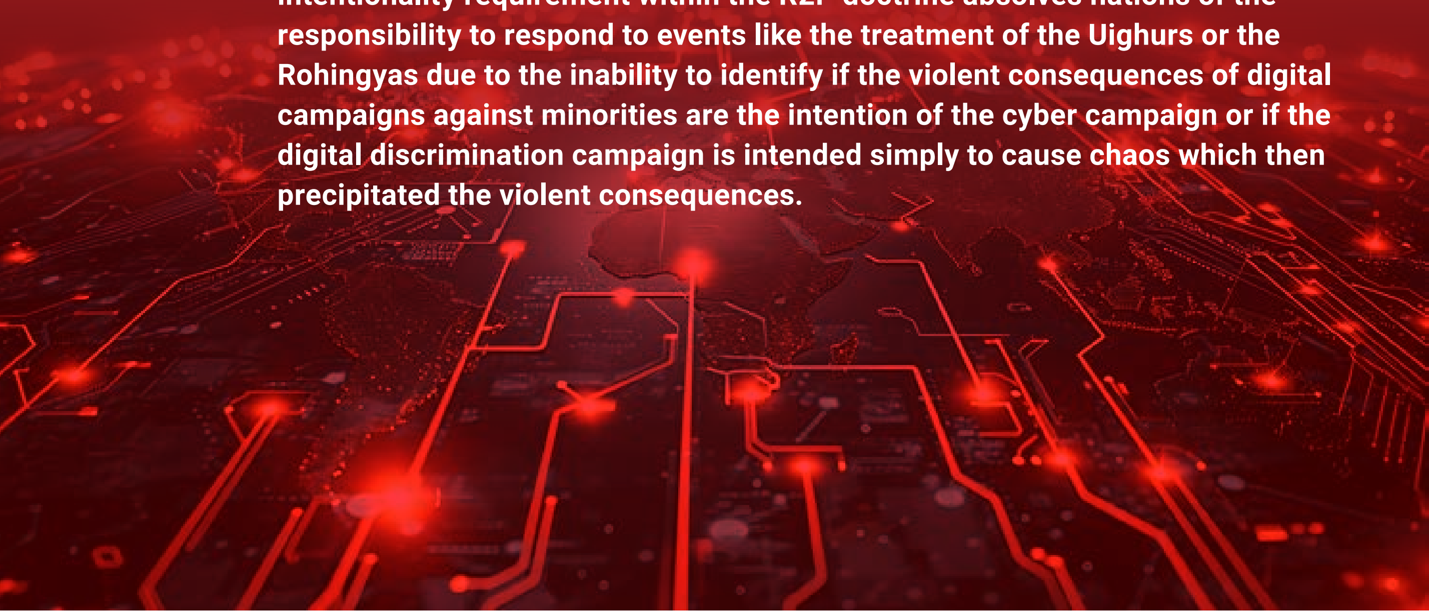
[51] A. Roy, "The Indo-Pacific Partnership for Maritime Domain Awareness," *Pacific Forum,* accessed April 1, 2024, https://pacforum.org/publications/pacnet-48-a-work-in-progress-the-indo-pacific-partnership-for-maritime-domain-awareness/.

on the state of sea lanes of communication in the Indo-Pacific. However, the realities of expensive commercial satellite imagery providers, poor nations, and technically non-interoperable fusion centers, each run by separate authorities, have hindered progress.

Without overcoming these obstacles, a shared image of the operating environment in cyber and physical space will exist only sporadically and across fragmented networks of minds. In the event of a crisis, such a disjointed understanding of the base reality will lead governments and armed services to independent conclusions, which may result in disaster.

Box 5 - Digital Discrimination and R2P

Digital discrimination is part of the reality of a digital world and the impact on an individual or minority group can be extremely significant. The Uighurs in China's western Xinjiang region face extreme digital surveillance that is tied to unjust incarceration, relocation, or internment in an indoctrination camp. Myanmar utilized the Chinese treatment of the Uighurs as inspiration for the treatment of their own religious minority, the Rohingyas, in a Facebook campaign that led to violent mass rape, forced migration, and genocide.[52] Redefining the shared responsibility under the R2P doctrine may be necessary to address these types of events more directly. Currently, the intentionality requirement within the R2P doctrine absolves nations of the responsibility to respond to events like the treatment of the Uighurs or the Rohingyas due to the inability to identify if the violent consequences of digital campaigns against minorities are the intention of the cyber campaign or if the digital discrimination campaign is intended simply to cause chaos which then precipitated the violent consequences.



[52] Michelle Lee, "Protecting Human Rights in the Age of Digital Surveillance: A Comparative Study of Rohingya Refugees and Uighurs in Xinjiang, China," SSRN, https://ssrn.com/abstract=4651223.

Recommendations

1. **The U.S. should reinforce the Indo-Pacific commons by expanding regional disaster relief, cybersecurity, and information transparency initiatives.** Writing in the 50s, Thomas Finletter observed that, "When people see alike, they become members of the same society…"[53] Working cooperatively to provide public goods is an effective way to build that 'same society' in the Indo-Pacific. To mitigate the strategic threat of natural disasters the U.S. should build up and maintain in-theater disaster relief resources. The U.S. should also explore a multilateral cyber defense/computer emergency repair team (INDOPAC-CERT) initiative to respond to regional cybersecurity threats for under resourced countries. Lastly, the U.S. should build on the momentum of the MDA and explore a multilateral information transparency initiative to proactively expose and monitor disinformation campaigns.

2. **The U.S. should supplement these public goods efforts with the Indo-Pacific cyber and conventional open-access intelligence clearinghouse (mentioned in finding 3).** Without a clear and shared operational understanding of the conventional and informational environment, de-escalation will be unacceptably dependent on chance and good fortune. Current intelligence clearinghouses range from military-specific classified mission partner environments at one end to public-private data fusion centers at the other, with a thicket of media and academic efforts in between.[54] The U.S. should take the lead in integrating government and private intelligence pipelines into a reliable open-access portal for allies and partners that provides reliable information and intelligence on the cyber and conventional domains.

3. **In this effort, the U.S. should prioritize incorporating intelligence and information flows that bypass classification silos altogether.** Generating buy-in to a commons approach to situational awareness will require a speed and generosity that legacy classification processes cannot regularly produce. Collaboratively producing the intelligence, surveillance, and reconnaissance platforms for this clearinghouse is one way to generate a trusted, responsive, and transparent information processing capability.

[53] Thomas K. Finletter, *Power and Policy: U.S. Foreign Policy and Military Power in the Hydrogen Age* (1st ed., Harcourt, Brace, 1954), 87. The rest of the quote reads: "...None of this is true in the Far East or Middle East."

[54] "Allies, Partners Tap into Technology to Monitor Maritime Domain," *Indo-Pacific Defense Forum,* November 14, 2023, https://ipdefenseforum.com/2023/11/allies-partners-tap-into-technology-to-monitor-maritime-domain/.

APPENDIX A – SUBJECT MATTER EXPERT INTERVIEWS

In the Delphi method of inquiry, experts are consulted for their opinions on a topic, much like an oracle that provides wisdom to the seeker. Threatcasting uses a modified Delphi process and seeks input from subject matter experts in various topics relevant to this study. Below are transcripts from interviews that were recorded by the Threatcasting team and presented as video clips to our workshop participants prior to them creating the effects-based models used as our primary data source.

These transcripts were machine translated from the video interviews. Light editing was conducted for ease of reading, but generally, the transcripts are presented here as our workshop participants heard them.

CHEN MINGQI

CEO, Institute for National Defense and Security Research

Hello, my name is Chen. I'm the CEO of the INDSR. Today I would like to take a few minutes to talk about cyber attacks and cognitive warfare against Taiwan. Cyber attacks are a growing global threat. While China is not the only country employing such attacks on others, it has certainly intensified cyber attacks and in the process strengthened its capabilities as the Chinese Communist Party under Xi Jinping increases its aggression against Taiwan. The People's Liberation Army or the PLA is also stepping up. Its cognitive warfare and disinformation campaigns are causing tension to rise in the Taiwan Strait and the PLA is a threat to the entire Indo-Pacific region.

There are some common tactics used by the CCP in its cognitive warfare against Taiwan. First, they aim to shape Taiwan's public opinion to undermine the government's credibility. For example, during the Covid pandemic, fake news about President Tsai and other political leaders secretly contracting COVID-19 went viral on social media. There were also propaganda posts with claims such as China offering to sell its COVID-19 vaccine to Taiwan but being rejected by the Taiwanese government. This information is spread to sew discord within Taiwan and make the public question our government's ability.

Second, they seek to undermine Taiwan's relationship with its allies and partners. Recently, we have witnessed a surge in fake news and disinformation depicting the U.S. as an unreliable partner for Taiwan, one that will withdraw its support for Taiwan if it suits its needs. Again, the CCP spreads this information to undermine the close relations between Taiwan and the U.S.

Third, to promote relations with China, the CCP conducts cognitive warfare to amplify the narratives they prefer to counter the U.S. and the West while solidifying domestic support for the rapid development of critical technology, especially AI. These raise the risk to Taiwanese cybersecurity as AI could allow China to radically improve and scale up its cognitive warfare.

Imagine a scenario where the CCP wants to create a rift between Taiwan's government and military. The PLA could hack into Taiwanese government servers and then use deep fake and related technology to create fake information about Taiwan's political leader distrusting the military. Or if they want to undermine Taiwan's relationship with the U.S. the PLA hacks into the server of Taiwan's Ministry of Foreign Affairs, and then releases the hack information online. Not only do they release the information, but they also mix the actual information with the distorted information about the U.S. government. Either scenario can happen, and if it does, it will greatly weaken Taiwan's resolve to stand firm against the Chinese threat.

To conclude, China is not only a threat to Taiwan, it is a threat to global democracies. As Chinese cyber attacks intensify, it is necessary for Taiwan to bolster its defenses. Doing so requires greater cooperation between Taiwan and other countries. Taiwan's extensive experience encountering Chinese cyber attacks makes it a crucial partner in protecting regional peace and security, including on the digital front. Thank you very much.

SHEENA CHESTNUT GREITENS

Associate Professor, Lyndon B. Johnson School of Public Affairs at The University of Texas at Austin

Thanks so much for having me today. It is a pleasure to be able to provide a brief for this exercise on cyber competition in the Indo-Pacific Gray Zone 2035. My name is Sheena Chestnut Greitens. I am a professor at The University of Texas at Austin, but for this year, I'm actually on leave at the Army War College at the soon to be launched China Land Power Studies Center working on the center launch and on various elements of our assessment of Chinese land power and strategy.

So, what I want to do today is talk a little bit about the strategic context in China's strategic thinking and particularly how that shapes its security outreach and cooperation in the Indo-Pacific. Many of you are probably familiar with some very top line debates that we've seen in the news about what China's strategy is, and the first question has to do with whether or not that strategy is new or different under Xi Jinping.

And so, you might have read a work like this book that says Xi Jinping's grand strategy is fundamentally similar to that of his predecessors, that basically this national rejuvenation strategy that Chinese leaders have pursued since Deng Xiaoping or at least since Reform and Opening in the post-Cold War period in the 1990s has really been unchanged, and that Xi Jinping is carrying that forward. So, they really emphasize continuity rather than change.

Then you'll see other folks who argue that there is more 'new' about Chinese grand strategy under Xi Jinping and that strategy is aimed at displacing the U.S. in the international system. And there's a lot of debate about what exactly displacement means. Does it mean that China becomes a leading power or the leading power?

But the point is that there's an active debate among people who read and watch China very closely about what China's strategy is. So, I wanted to answer that question because I think it's important for the workshop that you all are doing by basically laying out three criteria for whether Xi Jinping is doing something new and different. And that therefore, the security environment in the Indo-Pacific has fundamentally changed and will be different as we look ahead to 2035.

First, is there a different perception of the threat environment among China's leaders today than previously? Second, does the CCP adopt a different approach to address those threats? And third, does that new approach exist somewhere other than just on paper and in the heads and rhetoric of the Chinese leadership? Does it actually shape the force structure, organizations, and bureaucracy? Does it actually shape the legal infrastructure that governs how Chinese actors operate abroad? Does it shape personnel choices? Who gets appointed to run key positions and does it shape budgets and procurement and the actual sort of effort to put national power behind that strategy?

I would argue that for all three of these questions, the answer is yes, [which means] that Xi Jinping is doing something new and different that is changing the security environment in the Indo-Pacific as we look ahead to 2035.

So, in 2014, Xi Jinping launched what was called the comprehensive National Security Concept. And this was actually the concept that has framed and been used to organize a lot of the changes in the strategic landscape that we've seen during the Xi Jinping era, accompanied by the launch of a party body note. This is not a government body, but a party body called the Central National Security Commission that is designed to oversee and make decisions about national security policy. Now, the other translation of national security here is state security, and it's important to realize that this is fundamentally a regime security concept, which I'll come back to in just a moment.

Again, this has actually produced changes in the policy process. In January of 2015, the politburo approved the first ever national security strategy. Now, unlike the U.S. NSS, there is no unclassified version of the Chinese NSS that gets released to the public and the international community. We only know what the contents of the strategy are through official state media coverage. But we do know that in November 2021 the politburo approved a second national security strategy that covered the 2021 to 2025 period. So, this appears to be a sticky change in China's security policymaking process going forward. And we should pay attention to what we know about that strategy and look at what it tells us about how China perceives it and acts in its strategic environment.

One of the things it does is provide a different assessment of the threat environment in which China operates. Xi Jinping has said that China is now facing the most complicated—no, not the most difficult, [since] the CCP was almost exterminated during the Civil War—internal and external factors in its history, that its environment is marked by increasing threats and challenges. So, the picture isn't getting prettier for China, and these threats are interlocked and can be mutually activated. So, the CCP and China writ large have always seen a close connection between internal and external security. But Xi Jinping has sort of systematized and elevated the importance of this connection between external security challenges and the internal stability threats to the Chinese Communist Party. And I think it's important to note when you see phrases like 'major changes unseen in a century' and 'China approaching the center of the world stage', that can sound great for China, but in Chinese thinking, there's a dialectic at work, meaning that as China gets more powerful, it gets more opportunity, but it also has to bear more risk and confront more difficulty. And so, we tend to think of increased power as creating more security in some ways for China. The opposite is true. The more powerful it gets, the less secure it gets, and the bigger the risks and the problems are. It's important to recognize that because it's not always intuitive to us as outside observers. Xi Jinping has then outlined a new approach.

Again, as I mentioned earlier, the center of gravity of national or state security work is explicitly internal. And the foundation is what the CCP calls political security, which it defines as the authority of the CCP leadership of China's socialist system and of Xi Jinping at the core. So, this is fundamentally different from the way that the DOD or the United States Army might talk about national security. It is the security of the Chinese Communist Party and its leadership, which, remember, makes up about 7% of China's total population.

This is why we see things like this expressed as the red line during the meeting in Anchorage between key U.S. and Chinese diplomats, where the thing that is sort of framed as the red line that can never be crossed is the governing status of the Chinese Communist Party and the system that it oversees. It's the Chinese Communist Party's hold on power. That's what can't be challenged— that's always the reference, that's the thing that has to be secured in Chinese security thinking. There's a real focus on preventiveness. So, a lot of actions that we see China trying to shape its international environment are designed to prevent the emergence of threats to the CCP's hold on power at home.

The rise of the surveillance state is described as an information-based system for prevention and control domestically. And there are some other metaphors like immunization that again, really emphasize in Chinese discourse the preventive task that Xi Jinping has set for his military and security agencies. The other thing is that the CCP used to talk as if development would organically generate security. And the CCP's now framing it as developing security is the precondition for development, which means that generally China has been willing to bear higher economic and external costs if it thinks that a certain course of action will make it more secure at home.

So, these changes have actually been operationalized. And remember that's the third piece of the test I outlined for is this actually new and different? How much should we pay attention to this? Xi Jinping completely reorganized the national security apparatus that was true in the movement of the People's Armed Police. Under the Central Military Commission, it was true in the reorganization of the theater commands. And it was true in that he consolidated and restructured the way that the Party does discipline and supervision, which is the way he implements his anti-corruption campaigns and replaces a lot of personnel, including most recently, the folks at the top of the Rocket Force and the defense and foreign ministers of the PRC.

Xi Jinping has also pushed the National People's Congress, or prompted the National People's Congress, to lay out a completely new legal architecture for national security. And we see this continues up to today with this summer's passage of a new and updated counter espionage law. But this is just the first page of a two, now going on three, page list of regulations and laws that have been updated on national security in China. And the point again is just to make clear how sweeping and extensive the operationalization of these changes has been, the massive investment in tech procurement and the surveillance state on the domestic security side and in specific military civil fusion decisions on the military side. Also, again, these approaches really [require] a lot of financial weight to be put behind their implementation.

Then, there's the surveillance state itself. We sometimes read or think about it as a Chinese domestic phenomenon, but this map shows places that China surveillance platforms are being used by police and public security forces around the world, which is a large swath of the international community at this point. Personnel have also been significantly replaced. So, most of us have read at this point about the replacement of some of the folks in the military leadership as well as, we assume, of the defense minister. And that's applied to the internal security apparatus as well. So, there's been some very careful replacement of key personnel across both the military and the internal security forces, which are important. Again, because the reference is political security and regime stability internally. But there have also been some really important policy changes, and this is probably the most directly relevant.

I've tried to provide some of the conceptual backdrop to guide you all in your work today. But there have been some real direct policy changes in the Indo-Pacific and the way that China has engaged in the Indo-Pacific. The three big ones that I would note are the changing internal security strategy in Xinjiang, which has produced some outreach to Southeast Asia and the Middle East, in particular a growing emphasis on and prominence of counterespionage work. So, the Ministry of State Security now has a WeChat account, which is sort of fascinating and weighs in both on domestic counterespionage topics, but also occasionally on U.S.-China relations. So, it is both a domestic and, again, a foreign security communication platform. And then the final change is that PRC law enforcement activities [have] become heavily internationalized. So, military scholars for a long time, particularly the Naval War Colleges, the China Maritime Studies Institute, and NDU, have tracked the PLA and the PLA Navy's participation in military diplomacy abroad. But that's now been sort of augmented and complemented by outreach by PRC law enforcement.

In 2017, Xi Jinping urged the Ministry of Public Security to adopt a global vision in state security work. And the Ministry of Public Security has followed through on that exportation. This is a sort of screenshot of one of the big international conferences that China now hosts on the most recently. Yong Forum was actually held two weeks ago. And China hosts a range of law enforcement agencies from around the world to talk about its model of building a safe China. Sometimes there's a tech expo where Chinese companies can sell their products and their apps. And the Ministry of Public Security has engaged in a lot of police diplomacy heavily concentrated in Asia. So, you'll see in this slide on the right there, these are taken from an excellent report done by the Center for American Progress earlier this year. You can see that the bulk of the police diplomacy, even though they cover a lot of the globe, the frequency of activity is actually concentrated in the Indo-Pacific. So, it's important to think not only about what the PLA is doing, but also what the Ministry of Public Security is doing in terms of security cooperation and engagement. Because that also has, for your purposes and workshop, a significant cybersecurity component. This is measures of some other forms of ministry public security outreach, capacity building, meaning training, largely, and education, and then formal agreements either on police liaisons or extradition. And again, you can see that a fair amount of Southeast Asia is covered by these activities.

The final thing I'll touch on before I close, is something you may have read about recently, which is called the Global Security Initiative. It was announced in April 2022. It remains more a slogan than a set of concrete policies at this point, but it is clearly an effort to revise global security governance in two main ways. First, is to change the security architecture to bypass or create alternative mechanisms for handling security outside the American alliance and partnership network. China's been very critical of the alliance as zero-sum destabilizing, creating security for some at the expense of everyone else, and has really had a concerted messaging campaign, particularly in the Global South. And as it relates to both the Asian Security Theater and the European Security Theater, [China has emphasized] how detrimental the American approach is and how China's common inclusive vision of security will be better for everyone. It depends a lot on what that actually looks like in practice. And we don't have the details yet, so it's a little bit hard to offer a more detailed critique. But the other piece of this is that global security governance includes a pretty strong emphasis on what Xi Jinping has called non-traditional security threats. And those threats can often be addressed by the very outreach that the Ministry of Public Security has ramped up and has tried to increase in recent months.

The last thing I'll say is that the 20th Party Congress shows no sign of reversing course on this security. This is mentioned a lot. It has its own section in party documents for the first time and really codifies and elevates a lot of the statements that Chinese leaders have already made, elevates key people that Xi Jinping has identified as being able to implement and drive forward his approach. And so, there's really no sign that this approach is going to make a U-turn or pause or pull back at any point in the near future.

So again, a couple of implications here. Keep in mind as you're doing your work that the aim of whatever Chinese actors you're looking at or trying to assess is going to be to protect regime security as the Party defines it. And that internal instability is not necessarily going to lead China to pull back. In fact, if anything, it may escalate if it sees the causes of that internal instability as being fomented by black hands or foreign subversion abroad. (If you've got to be preventive and the cause is overseas, then you go get the cause and you actually amp up your foreign policy rather than retrenching.) A diaspora policy is likely to be heavily securitized. And reassurance will be difficult unless there's some reassurance that the United States or other actors can offer with respect to the Communist Party's hold on power. And I would say that that's both politically and morally pretty difficult to contemplate at this present juncture.

So, I hope that this has provided a good backdrop in terms of, you know, strategically how the CCP is thinking, what is it trying to accomplish, and what are some of the key assumptions that should guide your activities in the Threatcasting workshop. So again, I'm really pleased to be here and to provide this brief for you. Good luck and I look forward to hearing about the results. Thanks so much again for having me.

BRANDON KARPF[55]

Vice President and Executive Editor, N2K Networks
Adjunct Professor, Electrical and Computer Engineering, U.S. Naval Academy

***Prepared remarks in lieu of the transcript of Mr. Karpf's recorded interview.**

Threatcasting: The future of regional cyber threats in the Indo-Pacific

Executive Summary

Cyber threats in the Indo-Pacific region are escalating in sophistication and complexity. I'll outline several areas where the U.S. and our allies may fall short in meeting these challenges, as well as key domains where opportunities exist to make real inroads to address our cybersecurity challenges. The focus will be on six core areas: the current Naval force structure, the defend and hunt forward strategy, generative AI, cybercrime activity, industrial espionage, and the revival of agreements between the U.S. and nations in the Indo-Pacific region.

In any Pacific conflict, an effective and dominant naval force is crucial to an effective strategy. You need only to consider the region's geography to understand why. Our current naval force and manpower structure likely falls short in meeting the future challenges of the Indo-Pacific. Emerging drone technologies and affordable autonomous systems, akin to those deployed in the Ukraine conflict, introduce new strategic and tactical challenges that call for innovative approaches. Moreover, the Indo-Pacific is rife with territorial disputes,

[55] Prepared by Brandon Karpf. Email. LinkedIn.

which could worsen with the use of these technologies in contested areas.

Our defend/hunt forward strategy has been effective in detecting and responding to cyber threats. However, it's not a silver bullet and has several limitations. A major hurdle is the accurate attribution of cyber attacks. This is a significant issue in the Indo-Pacific region, with its many state-sponsored cyber actors and the political sensitivity surrounding attribution.

The rising use of generative AI in cyber attacks could pose formidable challenges ahead. These technologies can automate and scale attacks, rendering them faster, cheaper, and more effective. This might lead to a rise in the frequency and severity of cyber attacks in the region. Cybercrime groups, especially from Southeast Asia and North Korea, are a significant threat. These groups are growing more organized and sophisticated, capable of executing complex attacks against both public and private sector targets.

Chinese nation-state activities in industrial espionage pose a serious threat. China's long history of pilfering intellectual property and trade secrets from foreign enterprises continues unabated. This could significantly impact the economic and strategic interests of the Indo-Pacific region.

Moving forward, international agreements and partnerships between the U.S. and ASEAN nations are critical in addressing the future cyber threats in the region. These alliances can foster coordinated responses to cyber attacks, share crucial information and intelligence, and build capacity and resilience against future threats.

Key Findings

The Indo-Pacific region is home to some of the world's most important economies and strategic interests, and a major cyber attack could have far-reaching consequences. If we are not adequately prepared to meet these challenges, we risk ceding ground to our adversaries and undermining regional stability.

1. U.S. Navy Force Structure Limitations:

The Indo-Pacific region faces evolving unmanned and autonomous threats.

The U.S. Navy's force structure evolved over time to meet our strategic needs, adapting to technological advances and changing geopolitical realities throughout much of the 20th Century. The current structure, however, has been limited in adapting to modern challenges, particularly in the Indo-Pacific region, which is witnessing a rise in unmanned, distributed, and autonomous threats.

The current force structure was largely shaped by the necessities of large-scale naval warfare, embodied in World War II, and the subsequent Cold War era. This structure traditionally emphasized large, manned assets like aircraft carriers, destroyers, and submarines, forming Carrier Strike Groups and Expeditionary Strike Groups as the core of naval power projection.

The force structure has been guided by various naval strategies, including the "From the Sea" strategy of the 1990s, which shifted focus towards littoral operations, and the more recent Distributed Maritime Operations concept, which aims to distribute naval forces further across a wide area to enhance survivability and offensive capabilities.

However, the foundation of the current force structure is still shaped by various entrenched shipbuilding programs. The shift towards newer classes of ships, such as the Ford-class aircraft carriers, reflects the Navy's attempt to adapt to modern warfare, but it is still limited by its historic momentum around centralized command and control and the giant sexy jobs program that is the building and maintaining of massive manned vessels.

This system was designed in an era where manned vessels and aircraft were the primary assets, and the corresponding manpower was structured to operate, maintain, and protect these assets. The hierarchies, command structures, and operational doctrines were all framed within the context of these physical, human-crewed platforms, and the geopolitical realities of the time.

The rise of drones and autonomous systems, as seen in conflicts like the war in Ukraine, showcases how they will alter the strategic landscape. The effectiveness of Russia's Black Sea fleet has been largely neutered. Today, America looks a lot more like the Russian Navy than the Ukrainian Navy. There is no doubt that the Indo-Pacific region, with its many territorial disputes, will see these technologies employed in contested areas.

The current Navy force structure has a number of key limitations.

Meeting Regional Commanders' Requests: Challenges have been observed in meeting the requests from various regional U.S. military commanders for day-to-day, in-region presence of forward-deployed naval forces, particularly in the face of China's naval modernization efforts and resurgent Russian naval activity.

Adaptation to Modern Threats: The rise of drone and autonomous systems requires innovative naval strategies. Conflicts like the war in Ukraine have showcased how these technologies can alter the strategic landscape. In the Indo-Pacific region, these technologies could exacerbate many territorial disputes if employed in contested areas.

Inadequate Size of the Fleet: Advocates for a larger Navy point towards the challenges posed by China's naval modernization and other geopolitical factors as reasons to increase the planned size of the Navy beyond the current levels.

The current force and manpower structure is not sufficient to meet the future challenges of the Indo-Pacific region. The rise of unmanned and autonomous technologies, coupled with the naval modernization efforts of adversarial nations, requires a re-evaluation and possible restructuring of the Navy's force and manpower.

2. Defend/Hunt Forward Paradigm Limitations:

The Defend Forward strategy, which incorporates Hunt Forward operations, represents a contemporary approach to cybersecurity adopted by the United States and Cyber Command, spearheaded by General Nakasone. The strategy emphasizes engaging adversaries in cyberspace outside U.S. military networks to disrupt, degrade, or understand their activities before they reach our networks. Hunt Forward operations are a part of this strategy where U.S. Cyber Command personnel work with allies and partners to find and mitigate adversary cyber operations on their networks. This proactive approach aims to better understand adversaries' tactics, techniques, and procedures and preemptively address cyber threats.

Despite its proactive posture, the Defend/Hunt Forward paradigm has inherent limitations, particularly when applied to the complex geopolitical and cyber landscape of the Indo-Pacific region:

Difficulty in Attribution:

Attribution in cyberspace is inherently challenging due to the ease with which attackers can obscure their identities and operate from global locations. The Indo-Pacific region, with its myriad of state and non-state actors, further exacerbates this challenge. The difficulty in definitively attributing cyber attacks can hinder timely and appropriate response strategies.

Reactive Posture:

The Defend/Hunt Forward paradigm, while proactive in its operations outside U.S. networks, may still be reactive in nature when it comes to preventing cyber attacks before they occur. The paradigm is structured more towards understanding and disrupting adversary activities rather than preventing them from initiating these activities in the first place. Consider recent digital discoveries in Taiwan that many assume to be China's battlespace preparation activities.

Operational Constraints:

The operational execution of Hunt Forward missions requires significant coordination with host nations and other stakeholders. In fact, the host Nation must request, in writing, the provision of these forces. The legal, political, and operational constraints here may affect the timeliness and effectiveness of these operations, especially in a region with diverse legal frameworks and political sensitivities.

Technical Limitations:

The technical capability to detect, track, and mitigate sophisticated cyber threats is crucial for the success of the Defend/Hunt Forward paradigm. However, adversaries continue to evolve their TTPs, employing advanced evasion techniques, encryption, and other measures to avoid detection and attribution. We need to adapt just as quickly to be effective.

Information Sharing Challenges:

Effective information sharing among allied and partnered nations is essential for collective cybersecurity and defense. However, the varying levels of trust, differing legal frameworks, and disparate technological capabilities can hinder effective information sharing and collective action in the Indo-Pacific region.

Resource and Manpower Requirements:

The resource-intensive nature of Hunt Forward operations, which often require highly skilled personnel, advanced technical resources, and substantial coordination, are a limiting factor, especially when scaling operations across the vast and diverse Indo-Pacific region.

International Norms and Regulations:

The lack of internationally agreed-upon norms and regulations governing cyber operations can also pose challenges. The Defend/Hunt Forward paradigm operates in a domain where norms are still evolving, which can lead to misunderstandings and escalations if not carefully managed.

These limitations suggest that while the Defend/Hunt Forward paradigm provides a solid foundation for engaging cyber adversaries beyond national boundaries, there might be a need for augmenting this strategy with additional measures that are more deterrent in nature. These could include enhancing international collaboration, developing clearer cyber norms, investing in technological advancements for better attribution and threat prevention, and possibly exploring new operational paradigms to complement the Defend/Hunt Forward approach in addressing the unique challenges posed by the Indo-Pacific cyber landscape such as hack back or more clearly defined redlines.

3. Generative AI in Cyber Attacks:

In the context of cybersecurity, the potential applications of Generative AI are both promising and concerning. On the one hand, they could significantly enhance defensive cyber operations, threat intelligence, and simulation-based training. On the other hand, they also empower adversaries with more sophisticated attack capabilities. Some of which we're already seeing in the wild. For example:

Automation and Scalability: Generative AI has been used by attackers to automate the generation of malicious content and payloads, significantly increasing the scale and speed of attacks. By automating routine aspects of cyber attacks, adversaries could focus their human resources on more strategic, higher-level aspects of their campaigns.

Evasion and Obfuscation: Generative AI has been used to create malware that continually evolves to evade detection, making it extremely challenging for traditional security systems to identify and mitigate threats. Additionally, it could be used to generate misleading information or false indicators to obfuscate an attack, making attribution and response even more challenging.

Social Engineering Attacks: Generative AI has been used to create highly convincing fake audio, images, and text, which are used in sophisticated social engineering attacks.

Data Poisoning: Adversaries could employ generative AI to poison the datasets used to train machine learning models, subtly manipulating them to behave in undesired ways. This sort of attack could undermine the reliability and integrity of AI systems used in cybersecurity.

Impersonation: With the ability to mimic legitimate user behavior or create realistic fake identities, generative AI could be employed in advanced impersonation attacks, bypassing security measures that rely on behavior analysis or identity verification.

Resource Drain: And finally, defending against AI-driven cyber attacks could require significantly more computational resources and advanced detection technologies, leading to a resource drain for defending organizations.

Given the nascent state of generative AI and its potential to significantly alter the cybersecurity landscape, it's critical to prepare for the implications. Even just one year ago, none of us would have mentioned GenAI in this briefing. The rapid advancement of generative AI underscores the need for substantial investment in defensive cyber technologies to detect, counter, and mitigate these evolving threats. This includes developing new detection algorithms capable of identifying AI-generated malicious content, enhancing legal frameworks to regulate the use of generative AI, and fostering international cooperation to address the global challenges posed by the malicious use of generative AI.

4. Cyber Crime Groups in Southeast Asia and North Korea:

The Indo-Pacific region, particularly Southeast Asia and North Korea, has witnessed a growing sophistication and organization among cybercrime groups. These groups pose a significant threat to both public and private sector targets in the region, and pose a threat of unchecked conflict escalation when considering the challenge of attribution in cyberspace.

Southeast Asia: Sophisticated and Organized

1. Cybercrime groups in Southeast Asia are increasingly organized and capable of launching complex attacks against a variety of targets. INTERPOL recently highlighted that Southeast Asia is among the most actively targeted regions globally for cyber attacks, with business email compromise, ransomware, and malicious mobile applications being the top cyber threats.

2. In response, Australia has been fostering partnerships with Southeast Asian nations to combat cybercrime, reflecting the growing recognition of the threat these groups pose in the region, and a highlight to the sixth core area, international agreements and partnerships.

North Korea: State-sponsored and Persistent

1. North Korean state-sponsored cyber activities have included launching ransomware campaigns against Healthcare and Public Health Sector organizations and other critical infrastructure sector entities, showcasing a level of sophistication, focus, and indiscriminate targeting unlike any other nation state around the world.
2. North Korea's cyber activities are often financially motivated to bypass sanctions and fund their military programs. This includes targeting cryptocurrency firms and conducting cyber attacks for financial gains, destabilizing local financial systems and eroding trust in financial institutions.
3. North Korean cyber activities have also shown a recent shift in tactics, with hackers posing as journalists for spear-phishing campaigns to conduct cyber espionage around intellectual property as well as grand strategic positioning.
4. North Korea's cyber activities are coordinated through its military apparatus, signifying a high level of organization and state backing.

The growing sophistication and organization of cybercrime groups in Southeast Asia and North Korea require a holistic approach that encompasses international cooperation, robust legal frameworks, and enhanced cybersecurity measures to mitigate the threats they pose to the Indo-Pacific region.

5. Chinese Industrial Espionage:

The specter of Chinese industrial espionage remains a persistent challenge, particularly as the global landscape of technology and innovation continues to evolve. China has a long-standing and well-documented history of engaging in industrial espionage to further its technological and economic ambitions. The primary goal of these espionage activities is to accelerate China's economy, reduce its dependency on foreign technologies, and achieve a competitive advantage on the global stage. The tactics employed range from cyber espionage to human intelligence operations targeting a wide array of sectors including technology, defense, aerospace, and healthcare.

The Chinese government is often implicated in these espionage activities, either directly through state agencies or indirectly through proxies such as private companies, research institutions, or individual hackers. These actors are believed to engage in espionage activities that align with China's national interests, often at the direction of Chinese government officials, and they often target foreign companies and research institutions to acquire valuable IP and trade secrets.

Recently, we've observed that China is ramping up its cyber-enabled theft of U.S. intellectual property to advance its technological capabilities. The cyber dimension of industrial espionage remains a notable concern, and China's upper hand in this realm indicates a trend that's likely to continue being a focal point of contention between the U.S. and China.

The sectors often targeted encompass a wide array including semiconductors, telecommunications, aerospace, pharmaceuticals, and defense industries. The information acquired from these sectors is critical for China to reduce its technological gap, support its military modernization efforts, and achieve its long-term strategic objectives.

The ongoing geopolitical tensions, especially with the U.S., further exacerbate the concerns surrounding Chinese industrial espionage. The trade disputes and tech wars have often been linked to the allegations of IP theft, and this cycle continues to strain the relations between the two countries.

The existing legal and regulatory frameworks at both national and international levels often fall short in providing adequate measures to deter or penalize industrial espionage. The lack of a unified international stance and the discrepancies in national laws further complicate efforts to address this issue.

The response measures to mitigate the risks associated with industrial espionage are often reactive rather than proactive. Moreover, the coordination among different stakeholders including government agencies, private sector entities, and international partners is currently weak and unpredictable.

The persistent nature of Chinese industrial espionage presents a significant challenge that requires a concerted effort at both national and international levels to address. The good money is on this activity increasing in frequency and severity.

6. International Agreements and Partnerships:

Recent international agreements and dialogues have highlighted the importance of collective efforts to bolster cybersecurity in the Indo-Pacific region. Notably, the Quadrilateral Security Dialogue, also known as the Quad, involving the U.S., Japan, India, and Australia, has emphasized fostering a Free and Open Indo-Pacific through collaborative endeavors aimed at building cyber resilience, trust, and confidence in cyberspace.

U.S.-Japan Cybersecurity Cooperation:

Recently, the U.S. and Japan have underscored the significance of foundational cyber and information security consultations, reflecting a shared commitment to augment bilateral cooperation on cybersecurity matters.

U.S.-South Korea Cybersecurity Cooperation:

South Korea and the U.S. have agreed to elevate cybersecurity cooperation through various initiatives including regular cyber defense exercises, as per South Korea's Defense Ministry.

Trilateral Cybersecurity Relationship (U.S., Japan, South Korea):

The trilateral cybersecurity relationship among the U.S., Japan, and South Korea is driven by the mutual understanding of the economic and technological advancements of these nations, coupled with the routine experience of state-sponsored cyber threats from adversaries like China, Russia, and North Korea. The evolving cyber threat landscape necessitates a more integrated approach toward cybercrime-related information sharing and capacity-building efforts across these nations.

QUAD Cyber Cooperation:

The Quad, comprising the United States, India, Australia, and Japan, has expanded its cybersecurity cooperation to counter shared cyber threats. Recently, the QUAD Cyber Working Group shared its vision on fostering a free and open Indo-Pacific through building resilience, trust, and confidence in cyberspace.

On May 20, 2023, Quad leaders released a joint statement reinforcing their commitment to promoting a free, open, and inclusive Indo-Pacific, and to strengthen coordination in significant areas including cybersecurity.

AUKUS Partnership:

The AUKUS partnership, a trilateral security partnership between Australia, the UK, and the U.S., has broadened its focus beyond nuclear-powered submarines to include cyber capabilities, artificial intelligence, and quantum technologies. Recent developments in 2023 show a significant interest in enhancing cybersecurity cooperation to ensure a stable and secure Indo-Pacific region.

U.S.-India Defense Agreements:

The United States and India have accelerated the pace of signing important defense agreements and expanding military exercises, particularly in areas of cybersecurity, to rebalance the Indo-Pacific region.

U.S.-Philippine Armed Forces Cooperation:

The cybersecurity cooperation between the U.S. and Philippine Armed Forces also highlights the growing international partnerships aimed at enhancing cybersecurity in the region.

International agreements and partnerships between the U.S. and ASEAN nations are deemed crucial in navigating the future cyber threat landscape in the Indo-Pacific region. The collaborative stance adopted by nations within and beyond the Quad, alongside bilateral and trilateral cybersecurity agreements, signifies a concerted effort to coordinate responses to cyber attacks, share crucial information and intelligence, and foster capacity and resilience against looming cyber threats. Through such collaborative frameworks, nations aim to collectively address and mitigate the risks associated with the evolving cyber threat landscape, thereby contributing to the broader objective of maintaining regional stability and security in the face of adversarial cyber activities.

Implications

The implications of these findings are significant. The Indo-Pacific region is home to some of the world's most important economies and strategic interests, and a major cyber attack could have far-reaching consequences. If we are not adequately prepared to meet these challenges, we risk ceding ground to our adversaries and undermining regional stability. It is essential to develop a comprehensive and proactive approach to addressing these challenges.

NORI KATAGIRI

Associate Professor of Political Science and Coordinator of International Studies, Saint Louis University

My name is Nori Katagiri, and I am an associate professor of political science at Saint Louis University. I have a book forthcoming on the topic of how liberal democracies defend their networks from hackers through the strategy of active defense.

Here I discuss two challenges that Japan faces and extend the implications to the U.S.-Japan alliance. They're not really about typical DDOS, ransomware, phishing attempts because they've already been addressed by Japanese and Western vendors.

The first challenge is how to prevent the digital espionage of major politicians, bureaucrats, big firms in Japan, especially those with access to U.S. counterparts, by foreign and domestic agents who use various types of spying. I'm not just talking about spear-phishing but the use of advanced spyware programs, like Pegasus and Predator, which is very common in places like

Europe. This is because of the chronic shortage of social awareness by some elites and the technical challenge of blocking, detection, mitigation, and tracking of advanced technologies used for illicit purposes. The reason why this is a problem for the U.S.-Japan alliance is because of the lack of legal ban on spying programs and agents, widespread commercial use of these products, and some governments' condoning the use of these programs. Japan doesn't have an equivalent of the Espionage Act or Official Secrets Act 1911, so it has to use other laws to capture and prosecute spies, but because of that, sentencing is lighter than spying cases. So I'd say one of the opportunities for stability is to encourage your Japanese counterparts to strengthen anti-spy programs, although it may not be easy to do so because in the U.S., we already have lots of problems with them.

The other challenge is how to deal with AI-powered disinformation campaigns on Japanese policies, politicians, and other elites at critical times like national elections. I'm talking about various scenarios involving the use of deepfake programs, such as fake images of politicians and social influencers saying bad things about U.S. bases in Okinawa and U.S. military conducts in various parts of the Indo Pacific. The problem is that, like many other countries, Japan doesn't have regulations specifically designed to prevent the abuse of AI and software programs that control fake social media profiles. Some of these programs can be real threats because they can help hackers lower the language and cultural barriers they face when aiming at Japanese targets. And this one is hard to deal with because these technologies are growing much faster than regulation.

These are the major threats that I think warrant our attention at least through the year of 2035.

Jason Brown

Thank you, Doctor Katagiri. I have one follow up question. So, if you would, explain how the emphasis on politicians is such a critical node in international cooperation and partnerships with the U.S. versus surveillance of normal people, surveillance of banks and economies, and surveillance of social media. Why are politicians set aside as a critical node in your perspective?

Nori Katagiri

Politicians and bureaucrats, including those in the Ministries of Foreign Affairs and Defense, work hand in hand and share intelligence. I worry about lawmakers who are not keeping up with the threat environment and lack social awareness because they are just too busy with day-to-day issues. Their roles in the U.S.-Japan alliance remain critical, but they are also vulnerable to external efforts to undermine the protection of national security secrets.

TOSH MINOHARA

Chairman, Research Institute for Indo-Pacific Affairs (RIIPA)
Professor, Graduate School of Law and Politics, Kobe University

Hello, my name is Tosh Minohara. I am currently a professor of international relations and national security at the Graduate School of Law and Politics, Kobe University in Japan. I am also the chairman of the nonprofit Research Institute for Indo-Pacific Affairs (RIIPA). My academic interests focus primarily on U.S.-Japan relations, but this also encompasses modern Japanese and U.S. diplomatic and military history, foreign policy, and anything in between. I also possess a keen interest in national security issues, particularly as it pertains to the Indo-Pacific.

It is a real pleasure to be able to share my views today.

First of all, when we examine this region, we need to keep in mind that the term "Indo-Pacific" is a relatively new one. In the past, we generally used "Asia-Pacific" to refer to the region. But what makes Asia unique is that there's always been a traditional core in this region which is located in present day China, or what used to be called the Middle Kingdom. The Chinese character that we usually translate as "middle," also means "center." Thus, you can see that it perceived itself to be the center of the known world, and it did possess an advanced civilization on par with the Roman Empire. This is quite different compared to Europe, where the center of power would shift over time. China at the center of Asia was the norm for a millennium until the mid-19th century when the Europeans arrived. This led to the Opium Wars, which began the gradual decline of China as the preeminent hegemon in Asia. However, during the time that China was at the center, you had what was known as the tributary system. China was at the top, while the entity that controlled the Korean Peninsula at that time was generally considered to be in the number two slot.

On the other hand, Japan was viewed as a barbaric state that was out on the fringes. It would sometimes send a tribute to China, and other times it would completely disregard China. The combination of geographic distance and the security provided by the oceans allowed Japan to act in this manner. In the regard, it was sort of an outlier. The Chinese leader would sometimes get upset at Japan because the Japanese leader would send a letter addressed to the "King of China," from the "King of Japan" as though they were seemingly equals. Of course, the Chinese thought that this was completely ludicrous if not outright rude. What is really important to understand is that while a hierarchy existed in Asia with China at the top, but this hierarchy gradually began to erode with the rise of Japan in the late 19th century. The fatal blow for China was the 1894

Sino-Japanese War that ended in a lop-sided Japanese victory. Japan no longer perceived China to be the culturally and technologically advanced big brother. And in the 1930s, Japan's military expansion caused another major disruption, this time in the form of invading China proper.

...

We need to always keep in mind that history always flows forward; it's never static. In a greater time scale, great powers rise and fall. We've seen this with Spain, which was the first empire in which the sun never set. We don't view Spain as a great power today, but back in the day, it completely dominated, especially after the Iberian Union in the late 16th century. We can see still its impact because when you visit Latin America, people predominantly speak Spanish or Portuguese and are mostly Catholics. But again, history moves forward. Spanish hegemony was challenged by the up-and-coming powers of Britain, France, and the Dutch. Once they successfully brought Spain down, they bitterly fought amongst themselves until Britain emerged as the next dominant power, or hegemon. Thus emerged Pax Britannica. And looking at the diaries of their elites, it's clear that most believed that the sunshine over the British empire would continue for an eternity. But again, history shows us otherwise. But what was really unique about the British case is that since they had common values with the United States, they joined hands in maintaining the global order from 1917—America's entry to World War I—until 1945, the end of World War II. This is the period of the so-called Anglo-U.S. world order. And the eventual challenger to this order was Japan, Germany, and Italy, the trio was known as the Tripartite Pact, which later formed the core of the Axis powers.

The British and the Americans worked hand-in-hand to maintain the post-Versailles world order. You seldom see such cooperation in world history. Hence, this was a very unique case, which is also why it didn't last very long. After 1945, the U.S.—the only "true" victor in the aftermath of the second global war—became the sole de facto leader of the postwar order in the free world as Britain was in a state of shambles. We also shouldn't overlook that a vital American postwar objective was to not allow Britain to reestablish its colonies along with the ambition to remain the preeminent global power, that is uphold Pax Americana.

Well, what's happening today? We see the emergence of a 21st century tripartite alliance consisting of China, Russia, and Iran. You also have countries that are discontent with the current world order like North Korea, Venezuela, Cuba, Belorussia, Myanmar, Syria, so on. So, they will bandwagon with any major power that is willing to challenge the established order. Just last year at the Belt and Road Forum, Xi Jinping made it clear that he is seeking to establish a new world order. Vladimir Putin has said the same as well. It is interesting to see that Xi's rhetoric really resonates with the rhetoric that the Japanese were using in the late 1930s. The Japanese proclaimed a "New Order in East Asia," because they felt that the norms created by the Western powers were for their benefit only.

For example, the European powers possessed their vast colonies, but Japan was not allowed to expand and was limited in its overseas possessions. Also, there was the prevalent issue of racism. The Japanese immigrants were excluded from the United States as undesirable aliens in 1924. This was an action from a nation that espoused liberty, democracy, and equality. The Japanese were proud to have achieved so much in a such a short time, and, after 1919, Japan had become a so-called Big Five power. But this outright discrimination made them even more aware that they were the only non-White nation among the five. Essentially, there was a glass ceiling. Not being respected as a major power, at least from a racial perspective, led to resentment. Undoubtedly, when you look at the finer details, there are of course many differences between the 1930s and the present situation. But the basic game of wanting to alter the existing established order is exactly the same. In this way, history does not repeat but it rhymes—follows a similar pattern.

…

When you look at the history of Japan, you realize that during periods of strong central authority, known as bakufu, generally brought a period of relative stability with much fewer wars. However, during the phase in which the influence of the bakufu begins to wane, then domestic instability increases. A prime example is the decline of the Muromachi Bakufu (1336-1573). What followed was the turbulent era known as the Period of Warring States. Although this is a domestic analogy, I see this as a typical phenomenon when a global Pax wanes as well. As the current Pax, or the so-called hegemon, enters into a phase of relative decline, the world becomes increasingly more unstable. We saw this when Spain went into decline as well as when Britain went to decline. And today, I think most of us will agree that the United States is also in a state of relative decline. Perhaps that's why the slogan "Make American Great Again" resonates so much with a certain group of Americans. But even economic data shows that America is no longer great or dominant as it once was. United States' share of the global economy was 50% at its zenith, which is now about 24%. But in real terms, of course, the United States is still the most dominant economic and military power, and its population is increasing thanks to immigration. However, with the "rise of the rest," the United States is no longer dominating the world as it once did. The very fact that we now have a major war in Ukraine, the largest that Europe has seen since World War II, and that a major war is now looming in the Middle East, shows that Pax Americana is indeed gradually waning.

Conversely, if you have total dominance, wars generally are limited if they even occur. After all, the very definition of Pax is "peace that is enforced by a great power." But Paxes never last an eternity, and they usually begin to crumble from within. I don't think I need to show how completely divided the U.S. is at the moment as we witness a Congress that is struggling to function as it once did. Americans are completely divided as to what they perceive as an ideal nation. The list of the critical issues that lead to divisions is not short, beginning with abortion rights and gun control, etc. But as we bicker among ourselves, that forces us to look more inward and as a consequence the nation begins to lose its shine or appeal. Other countries no longer want to emulate us or look up to us. From the perspective of the other major powers that are displeased with the current rules-based liberal world order, a divided America creates a tremendous opportunity. They see a divided America as a weaker America, and they seek to exploit this weakness by increasingly challenging the United States on multiple fronts. But the only path to maintaining peace and stability is for these countries to accept the present U.S.-led world order, which means abiding by America's rules and values. I believe this is what President Obama was seeking with Xi Jinping. That is, he wanted China to become a responsible stakeholder in the existing world order. But this implied that a "value-sharing" China would become America's junior partner. But viewing itself as a great power with a history much longer and richer than the United States, China doesn't want to be anyone's junior partner.

Countries like Japan and most EU countries are very willing to be America's junior partner as they are not only like-minded, but they also depend on the United States for their security. This does not apply to China. Of the three countries that believe they are great powers—China, Russia, Iran—China in particular feels that it is at the cusp of regaining its historical dominance in the region. And if you see yourself as a great power, you will behave like a great power. But what is the fundamental definition of a great power? At the very basic level, it's much more than GDP or military prowess, but actually the strong will and desire to establish new norms which will allow the nation to pursue its national interests. In other words, a great power will in the end seek to establish a new world order to suit its liking. The economic and military capabilities provide the means to do so, and it is quite evident that China now feels that it has arrived at the stage where it's prepared to do exactly that.

…

Southeast Asia is undeniably a vital geostrategic area. But despite what many people in Southeast Asia proclaim, there is no true ASEAN centrality. The nations have conflicting interests, and they are divided over a host of issues. They conveniently come together only when they're facing a common threat. Each country in ASEAN is different in its own unique way, but one clear distinction is geography. I refer to this as maritime ASEAN versus land-based ASEAN. It's not really about whether you have access to an ocean or not, but rather the mentality that you possess. That is, how much value does your nation place on the maritime realm? Thus, I would include in the maritime ASEAN sphere Vietnam, Singapore, Indonesia, Malaysia, Thailand, the Philippines, and of course the giant in the region, Indonesia. These nations all have large coastlines and perceive open sea lanes as vital to their national interests.

These are also countries that have a vested interest—although the degrees differ—in the South China Sea and therefore view Chinese expansion as a real threat. Therefore, we should not engage with the entire ASEAN in the same manner but rather focus on the maritime ASEAN nations and make a concerted effort to draw them into our camp. The problem, of course, is that some of these are democracies and others are not. The Vietnamese, for example, have a "communist" government so they are ideologically more in line with China. I know that the military takes a very hard view toward China as they were not only occupied for a thousand years, but also fought a brutal war in 1979. But there are also many influential politicians who are pro-China, and view China as a political brother. So, what you have in Vietnam is a very messy picture. But we still need them as they are tough. Singapore is a very reliable like-minded partner. We shouldn't forget the Philippines either since they occupy a vital geostrategic location in containing Chinese expansion. Along with Japan, the United States is also currently expanding its security links with the Philippines. This is a new trilateral framework which will surely antagonize China.

We should seek similar arrangements with other maritime ASEAN nations with more vigor and urgency. Japan has a new program known as the Official Security Assistance (OSA). It's the security-focused version of the Official Development Assistance which was mostly about building bridges, schools, and other infrastructure. Now through OSA, Japan will be providing assistance to enhance the security of its regional partners, such as providing new Coast Guard ships and cutting-edge radar as it did for the Philippines in which it has signed a reciprocal access agreement (RAA). The world is rapidly changing, and you can see that Japan is trying hard to adapt to an increasingly hostile security environment.

...

One of the things that I firmly believe is that Japan needs to change is its security identity from being what I call a "security receiver" to a "security provider." Since the security treaty revision in 1960, Japan's identity has been one of being defended by the United States, essentially a "receiver" of the security that it needs. But due to the relative wane of Pax Americana, as witnessed by what's happening in Ukraine, the South China Sea, and now the Middle East, Japan needs to start seriously thinking of shifting from being only a security receiver—it has to be able to provide security as needed by the United States. I refer this new identity one of being a "security provider." What's really interesting, I've discovered through being in Japan and interacting with ordinary Japanese citizens and my college students, is that many are under the belief that Japan is not a large country and that it should strive to be a middle-power. I call this a "middle power mentality."

Of course, when comparing Japan to the United States, we see a nation that is area-wise smaller than California. But if we pick up Japan and drop it onto a map of Europe, it's larger, economically larger and has a greater population than France or Germany taken individually [and almost as large a population as both combined]. It would without a doubt be a core power of the European Union if Japan were actually situated in Europe. But the reality is that Japan is surrounded by two major powers: Russia and China. This makes Japan appear less significant than it really is, when in fact, depending on the prevailing exchange rates, it has the third or fourth largest GDP in the world. Although its population is shrinking, 125.1 million is hardly miniscule. So, we shouldn't expect Japan to behave like an Australia or a Canada that has only about a quarter of the population. But while these countries can afford to behave like middle powers, Japan cannot.

Japan has a greater responsibility in maintaining peace and stability in the region. And the key word is "region." I don't think Japan needs to be actively involved in the security affairs of Africa or the Middle East, but it definitely needs to proactively contribute to upholding the liberal order in the Indo-Pacific region, of which the most critical states are South Korea and Taiwan. These two countries are Japan's neighbor and having a hostile entity take over would gravely harm Japan's national interest. Despite all the historical disputes and other spats between Japan and South Korea, it's hard to deny that the liberal order can only be upheld if these two mature democracies work together; the synergy created would be tremendous.

A divided Japan and South Korea, on the other hand, only benefits China. Left-leaning South Korean presidents really didn't understand this basic fact. But now that South Korea has a realist leader who definitely grasps the big picture and thus understands that Japan is not only a friend but a strategic ally, there is momentum for these two countries to work closer together in the security realm and become a formidable presence in deterring Chinese expansion. Japan and South Korea can bring not only their respective military capabilities, but also the combined strength of the U.S. forces in both countries. A joint USFJ-

USFK-JSDF-ROK military is a formidable fighting force that possesses some serious deterrence capabilities. Therefore, we need to really take advantage of the situation now while there is a conservative leader in South Korea and a U.S. president who understands the importance of alliances in power. We also need to be more ambitious than the Chinese and not waste time in forming a U.S.-JPN-ROK alliance that combines with AUKUS, to become perhaps "JAUKKUS." Furthermore, we need to build upon the spirit of Camp David to ensure that Japan and South Korean relations don't backtrack especially as it relates to security issues. We should never forget that China can only win by changing the status quo. Therefore, they will surely move boldly to do so, and the only question is when.

When looking at all the security agreements that Japan has, the United States stands out as its sole true partner. Next to the U.S., Japan has what has evolved into a quasi-alliance with Australia. Japan is also actively expanding its security relations with Britain and the Philippines and forging closer security ties with the major NATO nations—as can be seen from the recent signing of Acquisition and Cross-Servicing Agreement (ACSA) with Germany and an RAA with Britain. Japan also has a Strategic Partnership Agreement with the EU and will be jointly developing its next-generation fighter with Britain and Italy. However, with Korea, Japan only has the GSOMIA—General Security of Military Information Agreement. This needs to change as Japan has to be able to check more boxes with South Korea and evolve the security relationship so that it rises to second place, only behind the United States in importance. If the Chinese were to move against Taiwan, the capabilities that these two nations bring together would be of critical importance to the United States.

In order to function together militarily, interoperability will be key, along with the military leaders of both countries being able to not only comprehend but also trust each other. This shouldn't be negotiated through the United States. Japan and South Korea need to be able to communicate directly and be able to work closely together even in the absence of the United States. This may not be a simple task, but nevertheless necessary, and the consultation pact that was formed at Camp David last year is an important step in the right direction.

Taiwan is the other crucial security area for Japan, but it has always been a very sensitive issue for both Japan and South Korea. Since they are so dependent on China economically, they are reluctant to upset China. But this doesn't mean that they can't make discreet and even indirect approaches to Taiwan. It's critical that Japan's admirals and generals know who their counterparts are in Taiwan on a personal level. As history shows us, this developed intimacy can be a key factor in attaining the upper hand militarily and can be accomplished in a very subtle manner. So, Japan should not be so reluctant in pushing the boundaries in forging stronger ties with Taiwan. One more thing that I strongly believe: Japan surely does not have any legal obligation to defend Taiwan, but as it had annexed the island for a half-century, it most definitely has a moral obligation to do so. And besides, losing Taiwan would adversely affect in a dramatic way, Japan's security realities in the Southwest (Ryuku island chain).

Finally, I'd like to touch upon the big variable: India. It's large and has surpassed China in population. It's also landed a rover on the south pole of the moon, a feat that has never been done before. They possess nuclear weapons. They've also surpassed Britain in GDP. So, it's clear that this country is really on the rise. Many Indians speak English and that's definitely an added competitive advantage. Furthermore, they are already a democracy. Of course, some are concerned with Modi's Hindu nationalism, but India still satisfies the basic criteria of being a democracy. Thus, they don't need to transition to a democracy, unlike countries such as Vietnam which will most likely eventually transition to a democracy, but this won't be easy.

Thus, India is definitely a global player, and it understands that it is indeed a major player. I have no doubt in my mind that India will have a much, much larger role in global politics by 2050. Maybe India will even be the next challenger to existing Pax, but I don't think we should be too concerned about a 2050 scenario at this time. We need to focus and properly deal with the present situation, in essence a 2030 scenario.

At this moment, it is clearly a lot better to have India in our corner. Of course, we shouldn't forget the possibility that India may become a future adversary, but that isn't now. Besides, India's path to becoming a great power is not a given as it has to overcome many domestic problems. For example, wealth has accumulated only to a very small percentage of the super elites and the caste system still exists though it's a lot stealthier now. In this way, they'll have to sort out a whole slew of domestic problems before they are even able to attempt to surpass the United States in becoming the next Pax.

CONGRESSIONAL TESTIMONIES

Our analytical team consulted the following additional testimonies and briefs to Congress for additional insights and trends. Excerpts from these testimonies were presented to our participants in the first phase of the workshop.

Cheng, Dean. “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States.” Testimony before the U.S.-China Economic and Security Review Commission, 2022.

Cary, Dakota. “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States.” Testimony before the U.S.-China Economic and Security Review Commission, 2022.

Vanderlee, Kelli. “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States.” Testimony before the U.S.-China Economic and Security Review Commission, 2022.

Shen, Puma. “China’s Global Influence and Interference Activities.” Testimony before the U.S.-China Economic and Security Review Commission, 2023.

Cook, Sarah. “China’s Global Influence and Interference Activities.” Testimony before the U.S.-China Economic and Security Review Commission, 2023.

Dunford, GEN Joe. “Department of Defense Posture and Budget.” Testimony before the House Armed Services Committee, 2018.

APPENDIX B – SURVEY OF CYBER-RELEVANT AGENCIES IN SELECT INDO-PACIFIC COUNTRIES[56]

Country	Cyber-Relevant Agencies and Departments
Australia	Australia Cyber Security Centre (within the Australian Signals Directorate), Joint Cyber Security Centres Program (JCSC), National Cybercrime Working Group, Information Warfare Division, Cyber Cooperation Program, Cybersecurity Operations Board
Japan	Cybersecurity Strategic Headquarters, Digital Agency, National Institute of Information and Communications Technology (NICT), Cyber Defense Group, Information-Technology Promotion Agency(IPA), National Center of Incident Readiness and Strategy for Cybersecurity(NICS), Information Security Council, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

[56] "Cyber Policy Portal," accessed March 31, 2024, https://cyberpolicyportal.org/ ; See also G. Harris, "The State of Cyber Defense Cooperation in ASEAN," *RealClearDefense*, January 31, 2024, https://www.realcleardefense.com/articles/2024/01/31/the_state_of_cyber_defense_cooperation_in_asean_1008628.html.

Malaysia	Ministry of Communications and Multimedia Malaysia, National Cyber Security Agency, Ministry of International Trade and Industry, Ministry of Women, Family and Community Development, Police Cyber Investigation Response Centre (PCIRC), Malaysia Digital Economy Corporation (MDEC), CyberSecurity Malaysia, Commercial Crime Investigation Department (CCID), Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), Malaysian Communications and Multimedia Commission, Special Cyber Court, Malaysia Computer Emergency Response Team (MyCERT), National Cyber Coordination and Command Centre (NC4)
Philippines	Cybercrime Investigation and Coordination Center (CICC), Department of Information and Communications Technology (DICT), Department of Justice, Office of Cybercrime, Anti Cybercrime Group (PNP-ACG), Philippine National Computer Emergency Response Team (CERT-PH), National Cybersecurity Inter-Agency Committee (NCIAC), National Intelligence Coordinating Agency (NICA), Philippine Cyber Command
South Korea	National Cybersecurity Center, Cyber Bureau, Korea Internet and Security Agency (KISA), Korea Internet Security Center (KrCERT/CC), Cyber Operations Command\
Thailand	Ministry of Digital Economy and Society (MDES), High-Tech Crime Division, Electronics Transactions Development Agency (acting National Cybersecurity Agency), National Cyber Security Committee (NCSC), ThaiCERT

APPENDIX C – DEFINING THE GRAY ZONE

The gray zone of ‘Cyber Competition in the Indo-Pacific Gray Zone’ has two overlapping but distinct elements: one functional and one geo-political. Functionally, the tactical and strategic use of cyberspace falls below established thresholds of conventional conflict and results in use-cases that defy existing understandings of competition and conflict. Geo-politically, on the other hand, the Indo-Pacific’s largely unsettled tangle of national interests are the primary theater of the ongoing strategic contest between the U.S. and China. The threat space our models revealed was animated by the interplay of both of these elements.

Nonetheless, the prevailing understanding of the term gray zone continues to focus on the functional over the geographic.[57] Interestingly, the American security strategists originally coming to grips with gray zones in the strategic competition that began in the 1950’s imbued the idea of ‘gray areas’ with a primarily geographic meaning. Credited with coining the term, Thomas Finletter, Secretary of the Air Force under Truman, described the gray areas as, “the long frontier between Freedom and Communism starting from Turkey on the west, and leading eastward through Iran, Afghanistan, Pakistan, India, Burma [Myanmar], Thailand, Malaysia, Indonesia, Formosa [Taiwan], Korea and Japan to the western limit of NATO in the Aleutian chain.”[58] This geographic use of the term was then taken up by influential theorists like Robert Osgood and Henry Kissinger before it was subsumed by the reemergence in the 21st century of the current functional understanding of ‘gray zone.’

[57] D. Stoker and C. Whiteside, “Blurred Lines: Gray-zone Conflict and Hybrid War—Two Failures of American Strategic Thinking,” *Naval War College Review* 73, no. 1 (2020).

[58] Thomas K. Finletter, *Power and Policy: U.S. Foreign Policy and Military Power in the Hydrogen Age*, 1st ed. (New York: Harcourt, Brace, 1954).