Marcellus
POLICY ANALYSIS

Spring 2025 - Marcellus Policy Analysis

Advancing a Restraint-Focused Cyber Strategy in the Indo-Pacific

By Joseph Brennan

EXECUTIVE SUMMARY

The Indo-Pacific is becoming the strategic hotspot of global competition where cyber power converges with increased geopolitical tensions, particularly between China and the United States. With digital technology embedded into military strategy, economic infrastructure, and everyday lives, cyberspace emerged as the area of contention and collaboration. The United States also faces growing threats from players with growing cyber capabilities in the region. These threats can vary from espionage and intellectual property theft to infrastructure sabotage and disinformation operations. Moreover, they are compounded by a lack of widely accepted norms governing state actions in cyberspace.

The emerging U.S. cyber posture places emphasis on proactive, disruption-based, and offense-capacity-building measures. Such means are desired but must be weighed against restraint-based policy. Restraint does not mean abandoning deterrence but reducing miscalculation probabilities, curbing escalatory spirals, and enhancing U.S. credibility as a responsible cyber power. In the Indo-Pacific, where democratic allies, emerging digital economies, and authoritarian upstarts overlap, a wisely weighted cyber policy based on defense, diplomacy, and multilateral norm-setting is needed to address long-term stability.

China’s Cyber Capabilities and Doctrine

China has emerged as one of the world’s most developed, assertive, and strategically aligned cyber superpowers. Its cyber strategy is deeply embedded in its total military, political, and economic objectives,

---

Joseph Brennan is an undergraduate at Seton Hall University studying International and Homeland Security, Data Analytics, and Cybersecurity. His interests are in grand strategy and cyber policy.

and is a keystone to its quest for overall national power. Unlike many other states that have treated cyber operations as distinct instruments, China has integrated cyber power into the very fabric of national security strategy, using it to advance state interests in peacetime, crisis, and in the gray spaces beneath war.

One of the most important developments in China's cyber evolution was the 2015 creation of the People's Liberation Army Strategic Support Force (PLASSF), which combined the nation's cyber warfare, electronic warfare, and psychological operations into a single military command. The PLASSF was a doctrinal and organizational shift toward "informationized warfare," wherein information domain superiority is seen to be essential to winning both kinetic and non-kinetic conflict.[1] The unification of these operations under the PLASSF facilitates integrated campaigns across the electromagnetic spectrum, facilitating greater intelligence collection, cyberattack operations, and psychological influence operations to shape perceptions and undermine adversary will. Although the PLASSF was discontinued, this "informationized warfare" doctrine has lived on through one of its replacements, the Cyberspace Force.[2]

Chinese military thinkers believe that the next war will not be won by simply having more firepower, but by dominating data, communications infrastructure, and mental space. This has pushed the development of dual-use systems that integrate civilian and military capability under China's Military-Civil Fusion approach, an all-of-nation initiative that mobilizes private tech companies, state-owned companies, and universities to create national security goals.

Operationally, China has deployed and built a portfolio of state-sponsored and state-authorized cyber units, most notably APT41, APT10, and Hafnium, that conduct a varied range of malicious cyber activities.[3] These encompass intellectual property theft, government and defense target espionage, cyber surveillance of dissidents, and supply chain implantation of malware. The Office of the Director of National Intelligence (ODNI) continues to identify China as the "most active and persistent" cyber espionage threat to U.S. national interests.[4] Such activity is not simply classic espionage but enables China to erode U.S. technological dominance and gain asymmetric advantages in sensitive domains such as aerospace, biomedicine, semiconductors, and artificial intelligence.

The economic burden of China's cyber-enabled theft is staggering. According to U.S.-China Economic and Security Review Commission reports, China's cyber behavior has caused the US economy to lose hundreds of billions of dollars in revenues, competitiveness undermined, and innovations stolen.[5] U.S. firms have been targeted for not only trade secrets but also weak internal information that may be used in future economic or political negotiations. These actions not only tilt the playing field of China's advantage but also attest to the strategic deployment of cyber tools as state-directed industrial warfare.

China's cyber strategy also includes robust controls for domestic governance and global influence. Domestically, the Chinese Communist Party (CCP) has constructed the world's most advanced digital censorship and surveillance system, the Great Firewall.[6] Through Huawei, Tencent, and Alibaba, many of which are subject to the law to support Chinese intelligence agencies under national security laws, Beijing gathers information on its citizens, monitors dissident groups, and suppresses information transfers.[7] Abroad, they are being traded. The CCP has launched an expansionist campaign abroad with mounting employment of cyber platforms in an effort to shape audiences, target journalists, academics, and diaspora communities in an effort to shape public opinion and silence critics. Human Rights Watch has documented pervasive Chinese surveillance of its overseas citizens and critics, including the use of spyware, social media tracking, and online harassment.[8]

Complicating the threat posed by China's cyber power is the use of strategic ambiguity deployments. As the Carnegie Endowment for International Peace defines it, this policy is a conscious component of China's policy that is intended to exploit cyberspace's diplomatic and legal uncertainties.[9] Rather than taking credit for cyberattacks, Beijing most frequently uses plausible deniability, proxy actors, and infrastructure masking to complicate attribution and dissuade counterattack. Through routing attacks through intermediate servers, the recruitment of support of non-state actors, or the utilization of commercial software, Chinese actors hide the origin of their

campaigns. The concealment has a twofold impact: it allows China to stay below the threshold of open conflict and prevents collective action attempts by the U.S. and allies.

The ramifications of China's overarching and impenetrable cyber doctrine are far-reaching. It erodes international confidence, makes norms harder to create, and increases the likelihood of accidental escalation in the event of errant attacks. For example, a cyber attack on Taiwanese or Japanese critical infrastructure by China without attribution, carried on in vague terms, could spur a forced response by the concerned nations or their allies, precipitating a larger regional crisis. Even a restrained American cyber posture in such circumstances would be overwhelmed by the quagmire of ambiguity created by China's operational modus operandi.

Regional Actors

The Indo-Pacific cyber realm should not be defined by great power competition of, for example, the United States and China. Rather, it is shaped by a constellation of regional actors whose policy, capability, and strategic direction all play a significant role in the overall security order. Australia, Japan, the Republic of Korea (South Korea), and Association of Southeast Asian Nations (ASEAN) countries are all important partners in building cyber resiliency, shaping regional norms, and engaging in multilateral cyber diplomacy. Their collaboration with the United States is critical to demonstrating a credible, collective resolve to address cyber threats in one of the most digitally dynamic and strategically consequential regions of the globe.

Australia has become a regional model for cyber defense through sustained investment and policy development. In 2020, the government released its Cyber Security Strategy that invested more than $1.6 billion over ten years to advance national cyber capabilities.[10] The strategy is centered on advancing critical infrastructure security, raising threat intelligence sharing, and building public-private partnerships. Australia contributes significantly to regional and global cyber threat analysis. Its emphasis on supply chain security and whole-of-nation coordination also aligns strongly with U.S. cyber policy priorities, and Australia is a natural collaborator on operational planning, threat reduction, and norms development.

Japan, too, has moved aggressively to advance its cyber posture in recent years, motivated in large part by growing alarm about Chinese and North Korean cyber activities. Its 2021 Cybersecurity Strategy addresses a broad array of national priorities that include enhancing cyber defense, leading digital economic growth, and building partnerships with like-minded nations.[11] Aside from investing in secure-by-design technology and governmental coordination, Japan is also reinforcing its national pipeline to meet the demand of the cyber workforce gap. Japan, with one of the most technologically advanced economies in the region, views its focus on public-private sector collaboration, threat intelligence, and infrastructure defense as standards in being a high-value Indo-Pacific partner in the overall cyber stability construct.

South Korea brings unique skill to regional cyber policy in light of its decades-long adversarial relationship with North Korea which is widely regarded as the world's most advanced prosecuctive cyber state. In response, South Korea has developed one of Asia's most advanced cyber defense systems. The Korea Internet & Security Agency (KISA) coordinates national resilience efforts, while South Korea's military Cyber Command also functions on the defense and offense sides as part of its overall deterrence effort.[12] Seoul's history with cyber attacks has seen its incident response protocols become more rapid and agile with strong legal frameworks, and growing international cooperation. Its three-way online coordination with Japan and the United States further acts to strengthen South Korea's role as a keystone partner in upholding digital stability in Northeast Asia.

The ASEAN member states provide a more complex and varied picture. While Singapore and Malaysia have improved considerably in their governance of cybersecurity, digital infrastructure protection, and human resource capacity, several of the other members of the bloc experience institutional limitations and low resources. The ASEAN Cybersecurity Cooperation Strategy 2021–2025 is a concerted effort to bridge these gaps through alignment of legal frameworks,

promotion of norms of responsible state behavior, and regional capacity-building.[13] The United States can and should be a force for good in promoting these objectives through technical expertise, funding for joint training programs, and diplomatic action through the ASEAN Regional Forum.[14] It not only improves cyber resilience across the region but also enhances a community of like-minded states which can validate commitment to open, secure, and stable cyberspace.

U.S. Cyber Command's Current Approach in the Pacific

The United States Cyber Command (USCYBERCOM), a unified command established in 2010, is the cornerstone of America's cyber posture. Its operational doctrine is built on the concept of "persistent engagement", which subscribes to the view that security in cyberspace requires constant contact with adversaries rather than reaction-based defense.[15] In this framework, USCYBERCOM is already active in disrupting adversary cyber activity at its origin by persistently engaging enemy networks, namely through the construct of "defend forward."[16] This strategy, officially adopted in the 2018 Department of Defense Cyber Strategy, enables U.S. forces to "intervene earlier," meaning to operate in gray zones before malicious activity reaches domestic targets.

Sustained involvement has been operationalized in initiatives like Hunt Forward Operations, in which USCYBERCOM deploys cyber teams to friendly countries at their request to discover vulnerabilities and intrusion detection in friendly networks.[17] Sustained involvement has been operationalized in initiatives like Hunt Forward Operations, in which USCYBERCOM deploys cyber teams to friendly countries at their request to discover vulnerabilities and intrusion detection in friendly networks. These operations have taken place in Ukraine, Estonia, Lithuania, and Montenegro, frequently in response to increased Russian cyber aggression. By alerting allies to their weaknesses and providing intelligence, such activities have yielded tactical dividends and strengthened cyber alliances. But the same model, transposed to the Indo-Pacific, a theatre characterized by a precarious balance of power and rising tensions, involves exponentially higher strategic risk.

The Challenges Persistent Engagement Would Face in the Indo-Pacific

In the Indo-Pacific, persistent engagement is riskier. Operating within or close to the networks of likely enemies such as China or North Korea would easily be perceived as preparations for offensive cyberwar. The Carnegie Endowment for International Peace warned that ongoing engagement has no clearly defined doctrinal boundaries and is typically performed covertly, thereby increasing the likelihood for strategic miscalculation.[18] The ambiguity over whether this activity amounts to defensive reconnaissance or offensive planning can lead U.S. enemies to misread American intentions and behave aggressively, particularly in a theater that is otherwise sensitive to nationalism and territorial concerns.

Also, sustained engagement raises serious questions about democratic control and accountability. Unlike traditional military action, much of this cyber war is stealthy and is being accomplished without widespread congressional approval or public debate. Such a lack of openness might erode policymaking trust, impede interagency coordination, and undermine U.S. credibility commitments to law and restraint in global conflict. While advocates for persistent engagement equate secrecy with effectiveness, critics point to the need for more visible legal boundaries, operational controls, and a more transparent doctrine that can be articulated consistently to allies and rivals alike.

There is also a question of sustainability and strategic prioritization. Long-term engagement takes vast amounts of resources, highly capable individuals, and a flexible command structure. With the expanding attack surface of critical infrastructure, domestic election systems, and supply chains, critics argue that offensive-first strategies may divert from other more important domestic cybersecurity needs. Moreover, continued activity fails to significantly address the underlying inherent systemic vulnerabilities of U.S. networks or improve the capacity of Indo-Pacific partners to defend themselves independently. At best, it can provide tactical disruption in the near term but not strategic resilience in the long term.

The Need for Restraint

A restraint-based strategy would imply a fundamental adjustment of USCYBERCOM's strategy in the Pacific. Rather than emphasizing forward disruption, a restraint approach would emphasize transparency, defensive capability-building, and closer collaboration with regional allies. This might include more comprehensive joint training exercises, synchronized vulnerability testing, and common threat intelligence foundations. It would also necessitate institutionalizing channels of communication with rivals to reduce the risk of accidental escalation and to entrench norms of acceptable behavior in cyberspace.

The ultimate objective, then, is not to dismantle USCYBERCOM capabilities but to redirect them on the strategic imperatives of stability, confidence-building, and prevention of conflict in one of the world's most significant regions. As the Indo-Pacific figures more centrally in global cybersecurity affairs, a more balanced, defensively focused, and diplomatically centered cyber strategy will be required to preserve peace and prevent the militarization of cyberspace.

Historical Precedents and Escalation Risks

The development of cyber warfare over the last twenty years demonstrates a concerning trend: apparently contained or secretive cyber activities have had unpredictable, disproportionate, and at times worldwide effects. These precedents highlight the pressing necessity for an approach to cyberspace policy that emphasizes restraint; one that accounts for the instability of cyber instruments, the uncertainty of attribution, and the potential for technical measures to ignite strategic instability with ease.

One of the earliest and largest scale is the 2007 Estonian cyberattack that has been nearly universally attributed to pro-Russian actors following a diplomatic dispute over the relocation of a Soviet war memorial.[19] Organized distributed denial-of-service (DDoS) attacks brought down government websites, banking, media, and other critical services nationwide for several weeks in what was described as the first case of a nation-state cyber disruption. Even though hardware infrastructure was not destroyed and nobody was killed, the assault brought a digitally dependent society to a halt and revealed how cyber means could be employed for geopolitical purposes. Estonia's experience was so bewildering that it served to spur the development of NATO's doctrine of cyber defense, including the establishment of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.[20]

The 2010 Stuxnet operation was a step towards offensive cyber with real-world implications. Suspected to have been a dual U.S.-Israeli operation, Stuxnet was designed to undermine Iran's uranium enrichment program by targeting programmable logic controllers on centrifuges.[21] While the operation was technologically sophisticated and very precise, its discovery acted to ignite global concern at the precedent set by the campaign. Stuxnet had shown that malware was able to propagate over air-gapped networks and result in real-world harm, dispelling the age-old notion that industrial networks were beyond the reach of cyberattacks. Moreover, it is also purported to have spurred other countries to develop such capability.

Among the most pervasive and indiscriminate cyberattacks ever to have been perpetrated was the 2017 NotPetya malware attack.[22] Launched by Russian state-sponsored hackers with the aim of destabilizing Ukraine, the malware spread quickly far beyond its original target, as it was self-propagating. Within hours, it crippled international companies Maersk, FedEx, and Merck, causing more than $10 billion worth of damages and disrupting supply chains and shipping networks around the world. NotPetya pushed the line between cyber war and economic sabotage. What was originally a concentrated geopolitical attack blew up into an international crisis that illustrated how cyber tools, relative to conventional weapons, are not necessarily defeasible in being confined to specific targets.

Even state actor cyberattacks have already proven able to engender cascading effects. The 2021 Colonial Pipeline ransomware attack perpetrated by the DarkSide cybercrime collective led to the temporary closure of the biggest U.S. fuel pipeline.[23] The result was mass panic purchasing, East Coast gasoline shortages, and a national state of emergency. Although

not entirely the product of a foreign government's efforts, the attack proved that civilian infrastructure remains a vulnerable target. Further, state-linked, or state-sponsored actors can leverage it to develop strategic repercussions disproportionate to the technical investment made.

These incidents share several characteristics in common that emphasize the argument for restraint. First, they illustrate the challenge of attribution. In both cases, initial confusion swirled around responsibility, means of attack, and whether a tit-for-tat response was warranted. Even when eventual attribution was made confidently, delay eliminated response options. Second, they illustrate the challenge of proportionate response. Responding too strong risks escalation; while responding too weak invites further incursions. Finally, they identify the risk of escalation of cyber operations, which, while kept within scope, tend to go out of control by infecting malware, targeting civilians, or by being misunderstood as to intent.

Restraining strategy avoids those dangers in a number of ways. By publicly announcing clear boundaries and prioritizing defense, the United States will be less likely to be perceived as a hostile-appearing actor and will encourage mutual restraint. Strategic transparency can even forestall misperception, especially when paired with international cooperation on incident attribution and de-escalation procedures. By highlighting resilience rather than retaliation, a restraint policy shifts the emphasis from blame and punishment to protection and recovery. In cyberspace, where the lines between war and peace are often obscured, such a dichotomy is invaluable.

Why Restraint Matters in Cyberspace

Strategic restraint in the online arena is not a reactive or passive creed: it is an active and proactive creed that prizes defense, stability, and long-term credibility of national cyber policy. In a realm where this space is characterized by obscurity, risk of escalation, and very little historical precedent, restraint provides a vital lens for managing uncertainty and mitigating the dangers of miscalculation. Penetrations in the digital sphere tend to blur the line distinguishing between espionage, sabotage, and preemption. In the absence of recognized thresholds of action and shared standards of responsible behavior, even small incidents can mushroom into international crises. Restraint under these circumstances is an agent of stability that can distinguish legitimate state action from aggression. Cyberspace poses special challenges for classical deterrence approaches. In the history of the world, punishment-based deterrence, founded upon the threat of retaliatory armed attack, has succeeded because the projection of force and attribution are clear. In cyberspace, however, attribution is a daunting challenge. Actors can hide behind third-party infrastructure, false flags, and proxies, so no one knows who to hold accountable. This imprecision slights both credibility of deterrence and the prospect of proportionate response. Deterrence by denial, therefore, which seeks to decrease chances of successful attack through target hardening and increased defenses, is a better and more resilient strategy.

The Center for Strategic and International Studies (CSIS) has argued that denial-based deterrence is particularly apt to cyberspace, where resiliency, containing an attack, and rapid recovery are given priority.[24] Rather than relying on retaliation which could possibly be undesirable, a firm denial posture deters attackers by raising the price of operations and reducing the expected benefit of doing so. This strategy is especially effective when coupled with public declarations of red lines and open attempts to bolster defense of infrastructure, communicating that the United States can and will defend itself without needlessly escalating. Restraint is also in line with international efforts to place norms in a box and reduce the threat of cyber war via multilateral collective action and diplomacy.

Multilateral bodies like the United Nations Group of Governmental Experts (UNGGE) and the Organization for Security and Co-operation in Europe (OSCE) have provided widely supported frameworks calling for the non-targeting of critical infrastructure, respect for sovereignty in the cyber domain, and resolution of cyber-related disputes through peaceful means.[25] America's adoption of a restraint stance would underline these principles so that Washington can set an example and augment its moral suasion in future norm-setting negotiations. This is particularly vital in the Indo-Pacific, where many states are still wary in respect to great power cyber behavior and

need to be confident that cyber competition will not make their own networks and institutions insecure.

Restraint is likewise essential to maintaining the fundamental principles of democratic accountability and civilian control. Offensive cyber operations tend to be classified, legally uncertain, and subject to minimal public scrutiny. This lack of transparency threatens to weaken public confidence, complicate interagency cooperation, and raise questions regarding mission creep and evasion of legislative authority. In contrast, a defense-centered, restraint-oriented policy based on international law, resilience, and defense leaves more room for institutional integrity, public discussion, and monitoring. Scholars such as Brandon Valeriano have emphasized that because "cyberspace is not offense dominant, but deception dominant," democratic governments bear a specific responsibility to ensure that cyber operations adhere to legal norms, avoid civilian harm, and remain accountable to the public and elected representatives.[26]

Finally, strategic restraint allows the United States to gain credibility among allies and competitors. By publicly announcing its cyber doctrine, limiting offensive action to clearly delineated and legal objectives, and avoiding gray zone activities that are likely to be viewed as escalatory, the United States can gain credibility and reduce the dangers of conflict misperception. It also facilitates partnerships by showing a commitment to multilateralism and cooperative governance in cyberspace that are values shared by most Indo-Pacific nations as they pursue their own digital transformation journeys.

Components of a Restraint-Focused Cyber Strategy

An effectively implemented restraint-based cyber strategy will have to be widely scoped, institutionally grounded, and operationally agile. Its success relies on merging three mutually reinforcing pillars: defensive cyber resiliency, escalation-free deterrence, and firmly established boundaries on offensive cyber action. Together, these supports not only protect U.S. assets and interests but also project credible, stable, and norm-led cyber conduct to friends and foes alike.

Defense cyber resilience is the linchpin of a restraint strategy. It rests on the theory that a protected and guarded digital infrastructure deters those willing to do it harm by diminishing the effect of their attempts, not by threatening back. At its core is the hardening of strategic infrastructure, such as power generation, water supply pipes, hospitals, transportation hubs, and voting systems, against cyber attack and sabotage. This must be pursued with strict compliance with advisories from the Cybersecurity and Infrastructure Security Agency (CISA), which emphasizes layered defenses, system redundancy, and recovery mechanisms in the event of failure.[27] Furthermore, implementing zero-trust architecture, as recommended by the National Institute of Standards and Technology (NIST), is required for ongoing authentication, access verification, and enforcing the least-privilege posture on government and critical private networks.[28] Zero-trust paradigms are particularly optimally suited to mitigate insider attack and attacker lateral movement, two of the most difficult vectors, historically, to protect against, in legacy environments.

Defensive resiliency also encompasses protection against the software supply chain, a large vulnerability highlighted in the 2020 SolarWinds attack, in which malicious code injected upstream taint a trusted software product utilized to infect multiple federal agencies.[29] To address this, federal software bill-of-materials (SBOM) requirements, secure coding practices, and third-party vendor monitoring need to be enhanced and put in place. Finally, a solid system is only as strong as the employees who work for it. The United States must close its persistent cyber talent deficit by investing in pipeline initiatives such as CyberCorps: Scholarship for Service, expanding training and upskilling, and improving public-private partnerships to share information and best practices.[30]

Cyber deterrence to avoid escalation is the second pillar, and it redefines deterrence as the activity of discouraging rivals by the credible denial of their intentions, and not by promising retaliation. In the cyber domain, where attribution is slow or indeterminate and retaliation threatens to unleash disproportionate consequences, this model is more realistic and more stabilizing. Effective deterrence begins with transparent and believable strategic communication. Asserting cyber red lines publicly, for example, prohibitions on targeting civilian infrastructure, election systems, or healthcare facilities, establishes normative limits.

To support this model, public cyberattack attribution has a critical role to play. When exercised with allies, collective attribution creates reputational and diplomatic risk for bad actors. For example, the joint U.S., U.K., and EU attribution of the 2021 Microsoft Exchange Server hack, wherein the actors were attributed as being linked to the Chinese state, shows how collective attribution can build up deterrent effect and international solidarity.[31] Deterrence is further supported by alliance-readiness, for example, by way of exercises, joint incident response planning, and cyber capacity-building programs run by institutions like NATO's CCDCOE.[32] These activities are not offensive but rather express readiness, enhance resilience, and offer a credible alternative to mutual unilateral offensive provocation.

Strategic restraint in offensive action constitutes the third, and most sensitive, element of the strategy of restraint. Offensive cyber capability remains an essential element of U.S. national security, but its employment must be carefully limited and governed by clearly established control mechanisms. In the restraint model, secret, or preemptive offensive cyber measures, particularly those potentially influencing civilian infrastructure, personal data privacy, or international diplomatic relations, would need to be subject to clear-cut restraints. These would involve legislative notice to relevant congressional committees and interagency determination prior to implementation. As the Cyberspace Solarium Commission has recommended, cyber operations should be evaluated by a clear risk framework that considers escalation potential, legal basis, operational effect, and unintended impact.[33]

Offense capabilities also need to align with U.S. international humanitarian law (IHL) responsibilities to discriminate, be necessary, and proportionate in all military actions. These principles apply in cyberspace just as they do in traditional warfare. Actions which have the potential to harm hospitals, water systems, or emergency response systems, either inadvertently or not, must be prohibited or brought under greater oversight. Respect for IHL in cyberspace helps not merely to legitimate U.S. action but also to establish a precedent which can influence global norms and allow for sustained long-term gains through credibility and moral leadership.

Misconceptions and Challenges of a Restraint-Focused Cyber Strategy

A policy of restraint in cyberspace offers a promising path to lasting stability and strategic credibility, particularly in competitive regions like the Indo-Pacific, but is met with both conceptual fallacies and implementation challenges. They stem from deeply rooted institutional practices, misperceptions about strategic intent, and the very nature of cyberspace.

The most common error is that cyber restraint signals weakness, undermines deterrence, and incites aggression. This type of criticism assumes deterrence is a function of credible threat and offensive power. However, cyberspace differs from traditional warfare in a number of significant ways, such as being marked by low observability, uncertain attribution, and covert action's tendency to escalate rather than deter. Public red lines, strong defenses, and restraint in offensive action, on the other hand, can reduce misperceptions and stabilize the situation. The 2015 U.S.-China Cyber Agreement, while short on detail, proved that diplomacy and commitments on both sides can contain malicious cyber activity, even from strategic competitors.[34]

But there is strong institutional resistance in the U.S. national security community. Groups like USCYBERCOM, the National Security Agency (NSA), and segments of the Department of Defense have long been advocates of continuous action and offensive disruption. A recentralization of restraint would require a cultural and doctrinal transformation, which might be perceived as diminishing flexibility or strength. Such momentum can be overcome only by top-down leadership from the President, National Security Council, and Congress to reset strategic priorities and enable interagency coordination.

Perception management is another critical challenge. Restraint, in the absence of transparent communication, may be misinterpreted by enemies as retreat or vacillation. To avert this, the United States must marry restraint with strategic communications that reinforce the hardness of its defense and the conditionality of its stance. Diplomatic engagement, cyber exercises, and alliances, like the Quad

Cybersecurity Partnership, can show that restraint manifests in principled leadership rather than weakness. Domestically, political leaders must articulate that cyber restraint enhances national security by minimizing chances of escalation and deepening democratic values.

Attribution challenges also undermine restraint credibility. Cyberattacks are often concealed by proxies and anonymization, which complicates the determination of aggressors and holds them accountable. Misattribution can lead to miscalculation or hesitant response. The U.S. must increase cooperation with international and non-state partners to improve threat intelligence and forensic capability. Such venues as the GFCE and Information Sharing and Analysis Centers (ISACs) can help establish standards, facilitate attribution, and capacity building across sectors.[35]

Public opinion, furthermore, renders a crucial advantage to restraint. A Pew Research Center survey conducted in 2021 found the majority of Americans to prioritize cyber defense and resilience ahead of offensive capabilities. When strategy is aligned with these values, domestic support for the underlying investments in infrastructure, workforce skills development, and digital literacy, the pillars of a resilient cyber environment, is created.

Regionally, Indo-Pacific diversity complicates harmonization on restraint. While allies like Japan and Australia have established cyber postures, the majority of ASEAN nations emphasize digital sovereignty or take risk-averse approaches to cooperation. Building consensus will require persistent diplomacy and context-specific engagement. Initiatives like the ASEAN-U.S. Cyber Policy Dialogue and Quad forums will have to be leveraged to align legal and technical standards, build confidence, and promote cooperation through capacity-building initiatives.

Notably, restraint is not the same as inaction. As Columbia University's Jason Healey explains, it is an assertive, self-restrained method founded on strategic vision and legal clarity. Establishing operational bounds enables the United States to enhance its moral legitimacy, strengthen accountability, and mobilize allies to respond to offenses. Restraint also enables a multi-faceted deterrence posture, combining denial, resilience, and diplomacy, to construct more durable and responsible cyber policy.

Policy Recommendations

In order to effectively implement a restraint-based cyber policy in the Indo-Pacific, the United States must undertake a sequence of interrelated, pragmatic policy measures that institutionalize restraint without sacrificing national security or international credibility.

First, the United States must revise its National Cybersecurity Strategy to formally enshrine strategic restraint as a fundamental principle.[36] Any revision should involve clear definitions of permissible state action in cyberspace, establish boundaries for thresholds of cyber involvement, and give precedence to deterrence by denial over deterrence by retaliation. By infusing restraint into national doctrine, the United States can heighten an international tone for engagement and increase domestic policy coherence.

Second, the United States needs to assume leadership in negotiating binding and voluntary cyber behavior norms through multilateral fora such as the ASEAN Regional Forum.[37] These talks need to focus on the non-targeting of civilian infrastructure, the establishment of channels of deconfliction, and increased openness in cyber operations. Diplomatic initiatives in these sectors would assist in building regional trust, minimizing chances of escalation, and fusing different strategic interests.

Third, restraint must be met with firm oversight and accountability mechanisms. This will involve heightening executive and congressional examination of offensive cyber operations, mandating post-operation effect assessments, and subjecting decision-making frameworks to civilian control and openness. An accountable operational approach will reduce the likelihood of miscalculation and ensure that cyber actions are consistent with U.S. ethical and legal standards.

Fourth, the United States must substantially invest in building regional cyber capability. Through collaborative action with organizations such as the Global Forum on Cyber Expertise (GFCE) and the Internet Governance Forum (IGF), Washington can advance legal harmonization, the development of

labor markets, and technical readiness among Indo-Pacific partners.[38] This would not only build collective strength, but also institutionalize U.S. leadership in establishing a rules-based digital order.

Finally, the private sector must be an equal partner in cyber restraint. The federal government must incentivize companies to adopt transparency best practices, develop secure-by-design technology, and participate in international norm-setting groups. As most digital infrastructure is owned by the private sector, public-private partnerships will be required to translate restraint into practice on the ground.

Combined, these five proposals form a roadmap for the addition of restraint to U.S. cyber policy that is realistic, successful, and responsibly global.

Conclusion

The Indo-Pacific is increasingly under threat from cyber threats that need strategic vision, diplomatic alignment, and robust defense. A cyber policy of restraint gives the United States a strategy to boost stability, reduce risks of escalation, and show responsible global leadership. Rather than displaying weakness, restraint affirms a commitment to peace, cooperation, and realistic deterrence.

Endnotes

1 Friedman, B. A. "Finding the Right Model: The Joint Force, the People's Liberation Army." *Air University (AU)*, 24 Apr. 2023, www.airuniversity.af.edu/JIPA/Display/Article/3371164/finding-the-right-model-the-joint-force-the-peoples-liberation-army-and-informa.

2 Bruzzese, Matt, and Peter W. Singer. "Farewell to China's Strategic Support Force. Let's Meet Its Replacements." Defense One, April 28, 2024. https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/.

3 "HAFNIUM, Operation Exchange Marauder, Silk Typhoon, Group G0125 | MITRE ATT&CK®," n.d. https://attack.mitre.org/groups/G0125/.

4 Office of the Director of National Intelligence. "ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY," February 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

5 U.S.-China Economic AND Security Review Commission. "2024 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION," November 2024. https://www.uscc.gov/sites/default/files/2024-11/2024_Annual_Report_to_Congress.pdf.

6 "China's Great Firewall," n.d. https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

7 Melnik, Jeffrey. "China's 'National Champions': Alibaba, Tencent, and Huawei." Association for Asian Studies, season-03 2019. https://www.asianstudies.org/publications/eaa/archives/chinas-national-champions-alibaba-tencent-and-huawei/.

8 "China's Algorithms of Repression." *Human Rights Watch*, March 28, 2023. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

9 Collard, Scott, Fan Yang, Jon Bateman, Xu Manshu, Ariel E. Levite, Lu Chuanying, George Perkovich, et al. "Managing U.S.-China Tensions Over Public Cyber Attribution." Edited by Ariel E. Levite, Lu Chuanying, George Perkovich, Fan Yang, and SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES. Uploaded by Carnegie Endowment for International Peace, n.d. https://carnegie-production-assets.s3.amazonaws.com/static/files/Perkovich_et_al_Cyber_Attribution_web.pdf.

10 Australian Government. "2023–2030 Australian Cyber Security Strategy." Common Wealth of Australia, n.d. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf.

11 The Government of Japan. "CYBERSECURITY STRATEGY," September 28, 2021. https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf.

12 Kisa. "KISA." KISA, n.d. https://www.kisa.or.kr/EN.

13 Brock, Julia. "ASEAN's Cyber Initiatives: A Select List | CSIS," n.d. https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list.

14 Asean Regional Forum. "ASEAN Regional Forum - Asean Regional Forum," April 17, 2025. https://aseanregionalforum.asean.org/about-arf/.

15 U.S. Cyber Command. "CYBER 101 - Defend Forward and Persistent Engagement," n.d. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

16 DEPARTMENT OF DEFENSE. "DEPARTMENT OF DEFENSE CYBER STRATEGY." *Department of Defense*, 2018. https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf

17 U.S. Cyber Command. "'Shared Threats, Shared Understanding': U.S., Canada and Latvia Conclude Defensive Hunt Operations," n.d. https://www.cybercom.mil/Media/News/Article/3390470/

shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/.

18 Collard et al., "Managing U.S.-China Tensions Over Public Cyber Attribution."

19 Keating, Joshua. "Who Was Behind the Estonia Cyber Attacks?" *Foreign Policy*, December 8, 2010. https://foreignpolicy.com/2010/12/07/who-was-behind-the-estonia-cyber-attacks/.

20 "CCDCOE - the NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise.," n.d. https://ccdcoe.org/.

21 Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *WIRED*, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

22 Stubbs, Jack, and Mattias Williams. "Ukraine Scrambles to Contain New Cyber Threat After 'NotPetya' Attack." Reuters, July 5, 2017. https://www.reuters.com/article/world/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14I/.

23 Cybersecurity and Infrastructure Security Agency CISA. "DarkSide Ransomware: Best Practices for Preventing Business Disruption From Ransomware Attacks | CISA," July 8, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a.

24 Lewis, James Andrew. "Deterrence and Cyber Strategy." Center for Strategic and International Studies, October 15, 2024. https://www.csis.org/analysis/deterrence-and-cyber-strategy.

25 "Developments in the Field of Information and Telecommunications in the Context of International Security – UNODA," n.d. https://disarmament.unoda.org/ict-security/.; OSCE. "Cyber/ICT Security," n.d. https://www.osce.org/cyber-ict-security.

26 Valeriano, Brandon, and Benjamin Jensen. "The Myth of the Cyber Offense: The Case for Restraint." Cato Institute, January 15, 2019. https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint#defense-and-deception.

27 "Critical Infrastructure Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA," n.d. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

28 Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. "Zero Trust Architecture," August 11, 2020. https://doi.org/10.6028/nist.sp.800-207.

29 Cybersecurity and Infrastructure Security Agency CISA. "Active Exploitation of SolarWinds Software | CISA," December 13, 2020. https://www.cisa.gov/news-events/alerts/2020/12/13/active-exploitation-solarwinds-software.

30 "SFS," n.d. https://sfs.opm.gov/.

31 Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency. "Compromise of Microsoft Exchange Server." Cybersecurity Advisory. *MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Framework, Version 8*, March 10, 2021. https://www.ic3.gov/Media/News/2021/210310.pdf.

32 "CCDCOE - the NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise."

33 "Cyberspace Solarium Commission - Report," n.d. https://www.solarium.gov/report.

34 Rollins, John W., Susan V. Lawrence, Dianne E. Rennack, and Catherine A. Theohary. "U.S.–China Cyber Agreement," 2015. https://sgp.fas.org/crs/row/IN10376.pdf.

35 "Home - the GFCE."

36 The White House. "National Cybersecurity Strategy | ONCD | the White House," May 7, 2024. https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/.

37 "ASEAN Regional Forum - Asean Regional Forum."

38 The GFCE. "Home - the GFCE," n.d. https://

thegfce.org/.; “Internet Governance Forum,” n.d. https://www.intgovforum.org/en.