ISSN Online: 3006-4708
ISSN Print: 3006-4694

SOCIAL SCIENCE REVIEW ARCHIVES
https://policyjournalofms.com

Sino-US Strategic Competition in Cyber Space Emerged as a Defining Feature of Contemporary Global Power Dynamics: An Analyses

Afzaal Amin [1], Dr. Zahid Ullah [2]

[1] Lecturer in Political Science GDC Lundkhwar & PhD Scholar Department of Political Science AWKUM Email: afzaal.amin92@gmail.com
[2] Faculty Member Department of Political Science AWKUM Email: zahidqau@gmail.com

DOI: https://doi.org/10.70670/sra.v3i4.1871

Abstract
Sino-US competition in the field of cyber space emerged as defining feature in the Global Political Arena. Both nations are giving prime importance to the matter and considered it as vital tools for the national security, Ideological influences and for the Economic Advantages. This rivalry encompasses the cyber espionage, the development of the offensive and defensive infrastructures and also for the intellectual property theft. China Cyber Policy Emphases on the cyber sovereignty and the state control over the flow of information while on the other hand the policy of USA is open and advocate the secure internet. This rise in the competition had intensified the tensions among the two nations and had deeply escalated the risk of cyber conflict. This competition had a deep sighted effect on the international norms and on the future governance.

Introduction

The US defines its cyber policy in a two-fold context of defensive defense and offensive deterrence, and each aspect does not rule out the other. This policy would guarantee the sanctity of the domestic digital infrastructure at the same time upholding the right to practice operations in the cyberspace to promote national security agendas (Shen, 2016, p. 6). The defensive part is comprehensive, as it is aimed at protecting the critical national infrastructure, including the energy grids, financial systems, and communication systems, against attacks. It includes both the technological fortification, such as the network segmentation and encryption, and the institutional implementation of the development of partnerships between the public and the private and the sharing of threat information (Ahmad, 2022, p. 11). Offensive capabilities, in turn, are presented as the key to deterrent, and policy statements explicitly provide the right to retaliate to cyber-attacks with a disproportionate force, which might include countering the origin of the menace (Shen, 2016, p. 6). The structure of defensive postures is focused on the idea of defending forward, which is proactive and does not seek to counter the adversary activities, but rather, to disorient them before they can reach the networks of the U.S. This approach includes searching the ill intent in foreign networks thus eliminating threats at their source. Such a forward leaning defense is further enhanced by the heavy integration with the allied capabilities and specifically with Japan. The revision of the 2015 U.S.-Japan Defense guidelines also explicitly proposes the seamless interoperability of bilateral cyber defenses, which expands the cyber defense capabilities of Japan, and gives the U.S. the freedom to concentrate on the offensive and retaliatory measures in the strategic front (Hughes and Kallender, 2016, p. 28). This has enabled Washington to exert power and dominate the world commons using allied networks and

intelligence. Moreover, the strategy is very focused on resilience and is aimed at ensuring that in case of a breach, the main governmental activities and vital services could be maintained. This includes the redundancy in systems, quick response to incidents, protocols, and constant drills that test the national preparedness such as the Cybersecurity and Infrastructure Security Agency (CISA). The deterrence by punishment is a declaratory policy that defines the offensive perspective of U.S. strategy, as opposed to such policies as deterrence by denial practiced by Japan (Hughes and Kallender, 2016, p. 27). There is a clear understanding of the fact that the United States can employ all tools of national power and cyber capabilities to retaliate against attacks, which was clearly stated in official documents, including the Department of Defense Cyber Strategy (Shen, 2016, pp. 56).

US Cyber Strategy

This right to self-defense is seen as much as possible, suggesting that network infrastructures in other sovereign states may be used as valid targets whenever it is necessary to address a threat. An interesting example of how this principle is implemented was in 2015, when the U.S. senior officials discussed publicly better retaliatory cyber efforts against China, following a massive data breach, specifically, with an aim of a deterrent effect since they publicly announced that they were able and willing to do it (Shen, 2016, p. 6). These revelations have a twofold effect, namely to convey determination to the enemy and to influence the way the U.S. cyber power is perceived both domestically and internationally. Both defensive and offensive postures are based on technological research and development (R&D). The U.S strategy focuses on speeding up advanced cyber R&D to develop advanced capabilities, paying more attention to increasing the capacity of the cyber mission force and the overall defense workforce (Sarker et al., 2019, p. 7). This includes channeling of basic and practical research in creating means of protection as well as exploitation. The investment in R&D guarantees the availability of a stream of developed technologies in detection, attribution, and response to maintain a qualitative advantage over the possible aggressors. But this technological dominance is not being sought all alone, they use this to build up alliance structures. According to Hughes and Kallender, the cybersecurity collaboration between the U.S.-Japan alliance makes it more likely that Japan will be pulled into collective self-defense on the cyber domain, as it has been in the case of maritime and air defense (Hughes and Kallender, 2016, p. 28). This gives the U.S. offensive choice greater strategic richness in terms of including resources of allies and geographic location. The equilibrium between the offensive and defensive is well balanced to not to escalate without being strategic in nature. The offensive operations are usually calculated and reversible so that the signaling could be provided without starting a spiral of uncontrolled conflict. The 2015 case against China represents the manifestation of such a measured response, and this choice in favor of partially public retaliation is indicative of it (Shen, 2016, p. 6). The U.S. aims to put red lines on the wall and define adversary conduct without having to engage in an outright cyber war by making some of its actions visible. On the defense side, the strategy recognizes that security at its utmost perfection is impossible, as a result, high resources are invested in attribution capabilities. Such rapid and plausible attributing of attacks is viewed as a foundation of deterrence because it diminishes anonymity which tends to embolden both state and non-state actors (Smith and Brown, 2021, p. 4). Investments into forensic tools and intelligence collection are meant to reduce the interval between an event and a certain attribution, thus responding to it faster and more precisely. To a state such as Pakistan, the way this U.S. strategy is observable is that of a cyber-super power that has an effortless match between an aggressive offensive stance and a strong homeland defense stance. The concept of integrating allies into its defensive system forms long chains of security that can become hard to access or manipulate by smaller states. At the same time, the powerful claim of a right to retaliate against sources of threats anywhere, including other sovereign states, creates a precedent that can be used in the tense territories, which can complicate the security calculations of Pakistan (Shen, 2016, p. 6). This policy of prioritizing R&D and deployed indigenous technological progression in the U.S.

is completely contrasted with the problems that Pakistan has to contend with, including the excessive reliance on imported hardware and software that adds to cyber risk (Ahmad, 2022, p. 10). Though the U.S. strategy provides a detailed roadmap to a secure cyber ecosystem based on institutional design and general awareness, the same goals are reflected in the National Cyber Security Policy of Pakistan (Ahmad, 2022, p. 11), the gap in the number of resources and technological background will be enormous, and the implementation process and the final success will be so different.

Institutional Structures to Cyber Security.

Cyber security institutional frameworks in the United States have evolved into a multi-layered system of multiple agencies, coordination that is allied, and policy oversight bodies that jointly carry out the domestic defense and international engagement roles. This architecture is a manifestation of the two priorities mentioned above in Section 4.1.1, in which resiliency of national systems need to coexist with the ability to make forward operations. The department of defense (DoD) takes center stage, with its strategy of cyber (2018), highlighting the inclusion of cyber capabilities in the general national defense plans (Shen, 2016, p. 6). The internal organization of the DoD consists of specific cyber mission forces whose area of activity extends to protecting military networks, assisting civilian infrastructure in case of major incidents, and initiating offensives in the situation with authorisation based on strategic directives. Under the purview of DoD, the U.S. Cyber Command (USCYBERCOM) is a single command that is charged with the responsibility of not only defending its digital network but also ensuring the offensive action is planned. USCYBERCOM is inextricably connected with service-specific elements, Army Cyber Command, Navy Fleet Cyber Command, Air Force Cyber Command, which retain domain-specific knowledge and operational preparation to deal with threats that are relevant to their respective theatres. These service aspects make it possible to customize the application of defensive actions, and they are also able to be integrated into combined campaigns; in such a case naval cyber forces can liaise directly with the operations of the fleet to stop maritime communications or disrupt enemy networks that affect naval logistics. Beyond the military domain, the Department of Homeland Security (DHS) via the Cybersecurity and Infrastructure Security Agency (CISA) is the key civilian institution of providing the security of critical infrastructure sectors that are considered vital to the functioning of the population (Ahmad, 2022, p. 8). CISA has programmes involving energy grids, financial systems, healthcare facilities, and transportation networks, with each sector having its Sector Risk Management Agencies (SRMAs) to establish particular security measures and to work with the operators in the private sector. The feature of the partnership between the government and companies is also typical of this case: CISA publishes threat intelligence through classified channels in de-anonymized fashion that allows business organisations to enhance their security without disclosing sensitive sources and techniques. Legislative oversight functions are another constituent of the institutional structure represented by Congress in committees that serve the homeland security, armed services, and intelligence functions. These entities consider the implementation of cyber policy, budgetary allocations towards capability building and the adherence to international commitments in the international forums (Ahmad, 2022, p. 11). Monitoring goes beyond finance to the assurance of conformity to doctrine, such as whether new deterrence measures adequately consider asymmetric threats by non-state actors that do not necessarily operate within the conventional paradigm of warfare. The National Security Council (NSC) is an interagency group that oversees interdepartmental strategic orientation. The NSC cyber directorate incorporates diplomatic posture within the Department of State with law enforcement coordination through the Department of Justice, FBI Cyber Division and technological policy contribution through agencies such as NIST (National Institute of Standards and Technology). Such an arrangement allows coherent national positioning in interacting internationally on cyber norms or in publicly attributing an attack. External agreements like the ones made during bilateral negotiations with allies, like Japan are reviewed at each of these institutional levels before formalization (Hughes

& Kallender, 2016, p. 28). Of key importance in this structure are the incident response mechanisms which operate at different levels of escalation. The National Cyber Incident Response Plan establishes the steps to follow in determining the affected sectors, mobilization of the agencies, deployment of technical teams including the US-CERT (United States Computer Emergency Readiness Team), and coordination of the remediation process (Ahmad, 2022, p. 8). In military scenarios, the protocols of incident response are directly connected to operational readiness requirements; the recognition in a closed system sparks an emergency response of isolating and investigating the incident under military chain of command jurisdiction. This two folds makes it fast to contain and consistent with wider deterrent communications in case attribution results in public release of investigative findings. International institutions supplement the domestic systems by integrating the U.S. participation into the multilateral frameworks of governance (Zhou, 2023, p. 2). The example is that liaison offices are bridging U.S. agencies to forums such as ASEAN Regional Forum cybersecurity tracking or ITU technical committees where the standards which relate to encryption or routing policies are discussed. Being present here will ensure control of technical specifications that will directly impact the interoperability of allied systems, which is a strategic requirement due to the collective operations envisioned by collective self-defense requirements (Hughes and Kallender, 2016, p. 28). Government-related research institutions also play the structural functions in this architecture. DARPA (Defense Advanced Research Projects Agency) does long-term research and development of technologies such as automated vulnerability detection, resilient network architecture aimed at contested environments (Sarker et al., 2019, p. 7). The result of outputs is fed back into operating bodies via pilot programs or capability transfers once developmental milestones have been achieved; this will continuity of conceptual innovation and applied defense posture and minimize lag time between the discovery and implementation of the discovery to field conditions. Legal compliance units in these institutions make sure that there is compliance with the domestic law frameworks such as FISMA (Federal Information Security Management Act) and that the operational requirements are aligned with the international applicable legal instruments Section 3.3.3. This in practice demands a strike between transparency requirements imposed by the rules of public accountability and secrecy requirements of national security operations, and this balance is often mediated by a judicial review procedure that preconditions attribution information disclosure when making public statements about hostile actions (Smith and Brown, 2021, p. 4). The structural complexity of institutional structures provides some degree of redundancy: in case a part of an institutional structure is compromised, either through technical violation or political interference, other segments can temporarily perform some of the functions of the system to avoid disintegration in critical times. But there is also associated friction; similar jurisdiction between the civilian apparatus of DHS and the defensive prerogative of DoD could introduce delays in coordination unless there were pre-established integration guidelines that are strictly followed during an incident in multiple sectors (Ahmad, 2022, p. 8). Resolving these frictions resulted in frequent joint exercises that simulate mass attacks on civil-military infrastructures; these exercises help familiarize each other with procedural peculiarities that eliminate the reluctance to take essential measures when faced by the reality of a threat. Through the eyes of the Pakistani regarding the witnessing of these arrangements, the potential duplication of even a part of the military and civilian cyber defense frameworks may greatly contribute to preparedness during danger due to the rivalry of the giant powers (Ahmad, 2022, p. 11). However, the limitations on resource allocation are challenges: keeping the individual, but interoperable institutional arms requires a long-term commitment to staff education, technology acquisition pipelines not subject to the threat of exploiting the supply chain, and legislative flexibility that can modify definitions of the sectors of infrastructure that are protected in accordance with the changes in the threat environment that is deeply embedded in the existing cyber security architecture in the United States.

Legislative and Regulatory Framework.

The statutory and regulatory framework of the U.S. cyber policy is a stratified structure that incorporates the statutory requirements, executive directives, and regulatory compliance structures into a coherent system of national defense and global interaction. This system is in keeping with the institutional frameworks outlined in Section 4.1.2, which ensures that operational agencies are legally bounded, subject to control and staffed with procedural directives on the domestic and cross-border operations. Fundamental legislation such as the Federal Information Security Management Act (FISMA) that establishes minimum security requirements to the federal information systems is foundational. FISMA requires periodic risk assessment, implementing minimum security controls, and ongoing monitoring, tasks that are spread among departments and directed by the overall agencies, such as the Office of Management and Budget (OMB) to coordinate policies on the same. It has authority over all executive branch agencies, which then have to keep certified incident response, contingency operations, and disaster recovery plans in accordance with national cybersecurity goals. In the same direction as FISMA is the Cybersecurity Information Sharing Act (CISA), which is intended to codify the mechanisms of information sharing on threat intelligence on both sides of the public-private divide. CISA offers liability coverage to companies sharing pertinent cyber threat indicators or defense with federal governments since most critical infrastructure in the United States is privately owned. This has increased the programs that are operated by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) to incorporate programs by the private-sector situational awareness into the wider national risk assessment model. Executive orders play a big role in the regulatory posture, as they guide the responses on the agency level to the changing threats. As an example, the Executive Order 13636 on Improving Critical Infrastructure Cybersecurity required the framework of risk management practices which can be voluntary as the National Institute of Standards and Technology (NIST) Cybersecurity Framework but offers templates of risks management to the sectors (Ahmad, 2022, p. 11). These frameworks are not mandatory but are highly embraced because they are recommended by regulators and industry organizations; they assist in standardizing essential procedures like the identification of critical assets, identification of anomalies, effective response, and recovery of incidents without causing permanent damage. These general statutes are overlays with sector specific regulations. Compliance regulations such as the Safeguards Rule of the Gramm-Leach-Bliley Act that regulates financial services and data protection of customers, the healthcare sector with HIPAA security regulations to protect electronic health records, and the energy industry with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) rules that touch on all aspects of SCADA system protection, including personnel training and physical access standards (Ahmad, 2022, p. 8). Every regime has a customized danger profile associated with its industry, the susceptibility of a hospital database is greatly different than the susceptibility of an oil refinery control system, but they have structural similarities based on the federal control and ultimately on the federal policy papers. The internationally facing elements of the U.S. legal framework consist of the laws of cooperation on cross-border computer crime investigation through the Mutual Legal Assistance Treaties (MLATs). These tools offer procedural language that gives acceptable evidence handling practices in different jurisdictions. In the presence of MLATs, as is the case with most NATO allies, they accelerate the process of data sharing when it comes to multinational platform or transnational hacker attacks (Zhou, 2023, p. 2). The lack of such treaties with some states would mean the necessity to rely on diplomacy or slower ad hoc measures, which would compromise quick response to high impact incidences. Export control laws also converge with legislative systems in such a manner that they form offensive capabilities indirectly. Distribution of dual-use technologies such as encryption software or intrusion tools is regulated by government authorities such as the Export Administration Regulations (EAR) that allow an item to be used both in a legitimate manner and in an unlawful way

(Du, 2023, p. 8). The U.S. law places itself as a gatekeeper to proliferation risks of advanced cyber tools by restricting exports, licensed under the condition of strategic alliances or geopolitical rivalries. Accountability is inculcated in this web of laws by the oversight functions. The congressional committees exercise jurisdiction in relation to homeland security, armed services, intelligence affairs, and commerce and each has a different vantage point of measuring the cyber readiness. Criminal cases on offensive planning as a response to opposing infrastructures entail the doubt not only of strategic necessity but also of legal feasibility in reference to current domestic laws and the relevant international standards Section 3.3.3. On the same note, approvals of budgets that are associated with the funding of a research and development must be established that research undertakings follow the ethical protection and do not contradict treaty commitments. The peculiar aspect of the U.S. legislative landscape is that it combines the mandatory compliance regimes with the voluntary adoption models which are promoted with the help of reputational benefits or a decrease in liabilities (Ahmad, 2022, p. 11). Indicatively, companies that show compliance with NIST Framework principles might benefit in the form of contractual favoritism in submitting bids to government contracts; the opposite might subject them to increased audit probabilities in the aftermath of major breaches. This transitional style allows flexibility but promotes uniformity of the baselines of the same which is pragmatic in understanding the diversity of organizational capabilities across sectors. Efforts to enforce it take the form of civil penalties by regulatory bodies such as the Federal Trade Commission (FTC), implemented due to insufficient consumer data protection by violators and criminal penalties where ill intent satisfies statutory definitions of criminal behavior under laws such as the Computer Fraud and Abuse Act (CFAA). The CFAA is one of the main prosecutorial tools against unauthorized access operations within domestic networks and can be applied to issues outside the country in case the systems of operators located in the United States are attacked (Du, 2023, p. 8). Supplementary clauses to wire fraud laws allow prosecutors to trace a connection of digital intrusions and financial damages when communicated messages are a component of fraudulent conspiracy. In the perspective of Pakistan that is witnessing these legislative trends, it teaches concerning the conjoined design of oversight. The implementation of comparable systems by CISA might enhance the capacity on the local level, meaning the ability to share intelligence among civil CERTs and the military security machinery that are considered as the impediments to national preparedness (Ahmad, 2022, p. 11). It also demonstrates some of the pitfalls; excessively restrictive export regulations or one-sided extraterritorial claims would make partners feel encroached upon in the event they seem like attempts to usurp sovereignty. After all, this legislative-regulatory grid can be understood as an intentional calibration between the need to protect core assets at home, display deterrent capability abroad, coordinate with allies when feasible on the same terms, and have unilateral freedom-of-action when it is necessary by strategic imperative (Du, 2023, p. 8). This balance is not static: legislative modifications are reactive to the changing threat vectors, and the executive orders are real-time changes to the focus of operations to maintain agility within the framework of the codified models that could be used to implement the comprehensive cyber strategy the U.S. defense doctrine envisions.

China's Cyber Strategy

Goals for Cyber Sovereignty

The expression of objectives of cyber sovereignty by China is simply a manifestation of a larger strategic plan, whereby dominance of digital territories will form part of the national security, political stability and world standing. Its idea is anchored in the fact that the cyberspace on the inside territory of China ought to be governed by the same laws of land and domestic control as the real space, therefore, giving the state the final power to control, observe and protect informational streams. This vision is connected to the long-term aspirations of the country to maintain the legitimacy of the regimes in the country and promote the alternative model of international order that is not rooted in

the Western-led standards of open and multi-stakeholder rule (Mokry, 2024, p. 4). In actuality, cyber sovereignty objectives include in-house unification and out-of-house framework Ming. On the internal front, Beijing is trying to make sure that the political leadership of the country has pervasive control on data creation, storage and sharing. It does not only require reacting to threats but proactively architecture that considers areas of critical control, like network gateway, as property or under the control of parties that are directly accountable to the state apparatus. This type of structural organization lowers the reliance on external platforms and averts unchecked movement of information in and out of the country that may harm local policy discourses (Zhou, 2023, p. 9). The ambition also stretches to construct strong indigenous technology stack that can be used to enable major functionalities of communication protocols and security standards without basing on proprietary technologies that are U.S.-aligned. This infrastructural level of control allows implementing the policies of content regulation and monitoring tools based on national priorities. These home designs are supplemented with clear codification of the law. The legal tools regulating network security focus on the concepts of information security and orderly internet development, with access control being viewed as both preventing the outside invasion and the regulation of the acceptable inner discourse (Mokry, 2024, p. 4). Such actions guard citizens against malevolent influence in the rhetorical frames of the Chinese government, which is adversarial phrased to encompass the actions that weaken a free and open order or promote other oppressive systems (Zhou, 2023, p. 4). This is seen by Washington as a claim to political supremacy which is destined to undermine the idea of liberal democracy in foreign countries, although in the eyes of Beijing is justified by putting digital governance in line with cultural values and political ideology which prefers state-directed orientation. Outside, cyber sovereignty objectives are projected into the creation of international cyber governance designs that can accommodate sovereignty-oriented preferences. The Chinese diplomacy frequently demands recognition on the multilateral level, such as the ASEAN cybersecurity programs or ITU technical committees where states hold the ultimate power of their own digital practices (Mokry, 2024, p. 4; Zhou, 2023, p. 9). The benefit of involvement in such venues is two-fold namely ensuring domestic regulatory latitude under international standards and facilitating technical standards in line with Chinese infrastructural design that would likely provide Beijing with competitive edge in case such standards become widely adopted. One of the recurrent themes is the connection between the goals of cyber sovereignty and the grand strategy like the provision of global public goods or global leadership in governance (Mokry, 2024, p. 9). Indeed, jobs focusing on sovereign control do not mean that it cannot be actively engaged abroad, in fact, China has been marketing itself as a source of stability by taking successful initiatives such as white papers outlining policy stands on foreign affairs but nonetheless inculcating its favored pattern of governance into collaborative structures. Particularly in Africa, widespread ICT infrastructure development goes hand in hand with the sale of governance norms aligned with the ideas of no strings attached, without conditionality's, which are aimed at strengthening the sovereignty-based forms of control (Sari, 2019, p. 12). These sovereignty objectives are pursued with greater competitive relations with the United States.

Integration with National Security Policy

The Chinese approach to integrating the cyber strategy with the overall national security policy can be viewed as a calculated coordination of the technological agenda, system regulation, and geopolitics-related goals. At the center is the realization that the domination of digital space is not only satisfying economical and industrial interests but also acts as the guaranty of political stability and responds to the internal opposition and the external pressure. This unification is based on the assumption that the cyberspace cannot be disconnected with such traditional theatres of security as land, sea, air, space, and should be included in the same strategic calculation as these other theatres (Сюаньцavia & Guaanya, 2024, p. 2). The doctrine of Chinese national security makes information

dominance a requirement to any successful operation in any confrontation. Cyber capabilities are built and implemented in a system of integrated military planning involving space-based reconnaissance, electronic warfare, and psychological operations (Katkova and Yunyushkina, 2022, p. 9). These are capabilities that constitute the People's Liberation Army (PLA) strategic support force that has the responsibility to determine the reliability of command-and-control systems in contested situations. In the case of Beijing, information control and disruption tools are part of defensive insurance that protects the infrastructures that are critical to the city against foreign infiltration and offensive capacity that can undermine the capabilities of the adversaries during crises. The national security need mentioned above relates to the scope of cyber sovereignty since, through legislation and infrastructural building under the supervision of the state authorities, national security is ensured. Laws require the localization of sensitive information in local networks to limit the exposure to foreign intelligence. This need is an addition to the military policies that presuppose that deterrence credibility could be undermined by vulnerability to foreign surveillance. As a result, China spends on homegrown technologies in artificial intelligence, quantum communications, cloud computing, and microelectronics (Сюаньцjpg & Гуаня, 2024, p. 3) to bridge the ability disparity with some of the world leaders such as the United States, without relying on imported systems that may have vulnerabilities to backdoors. In practice, integration is realized in the form of joint civilian-military exercises to simulate the coordinated work of the responses to cyber incidents and kinetic threats. Such situations equate infrastructure disruptions, which are a result of a hostile intrusion, with conventional sabotage in their severity of risk. Military formations working on computer network defense (CND) coordinate with non-military agencies such as the Ministry of Public Security in order to control technical countermeasures in the management of narrative flows on online media space to ensure that panic or politically destabilizing discourse in acute situations do not arise. This interdependence between such physical protection and management of informational environment helps to point out the dualistic essence of Chinese security planning: protecting not only material resources but the perception of the population against any attempts to manipulate or demoralize it in the cyberspace. The focus of informational warfare methods, such as computer espionage, control of the electromagnetic spectrum, and influence in China can be explained by its readiness to prefer non-armed confrontations in the event of a military conflict (Katkova and Yunyushkina, 2022, p. 8). Rather, the PLA doctrine promotes the ability to leverage weaknesses in enemy decision-making through pre-emptive sabotage of communication black holes or purveying of misinformation that will be adjusted to evoke a reaction to deployment. Such actions are not limited to military targets, but also include key economic centers of an adversary such as to its industrial capability, and is accepted internally as a key to overall security but is seen externally as unhealthy competition. The Taiwan case can serve as an example of applied integration: approaches to postponing U.S. deployments by disrupting their supply chain were presented as defensive contingencies in the planning of the work of the PLA troops (Katkova and Yunyushkina, 2022, p. 9), but they were carried out through the use of cyber tools installed on the inside of broader national defense systems. Another addition to the path of introducing cyber priorities into the national security policy is externally oriented projects such as Belt and Road Initiative (BRI) corridors (Sari, 2019, p. 3). Providing Chinese-constructed digital infrastructure in foreign nations, fiber-optic cables, data centers, satellite communications, the state increases its digital defensive perimeter virtually and, at the same time, allows it to monitor activities in major maritime bottle-necks and on land transport routes vital to resource-delivery lines. In Chinese strategic thinking, it has dual purposes of overseas ICT investments: not only are they allowing efficiency in trade but can be re-purposed quickly into facilitating roles in PLA operations in the event of a geopolitical stress along such lines. This assimilation supports the ability of Beijing to shield its outbound economic interests and plant control over the digital landscape of the host countries in a manner that supports its sovereignty ambitions

back home. The principles of cyber governance also affect the national counterterrorism efforts. Beijing concludes that it needs to moderate the terrorist utilization of online space in its land by combining the local policing roles with the international intelligence sharing but on terms that observe sovereignty standards it attempts to institutionalize in the international arena (Tehseen, p. 2). The actions are not only aimed at dissident actors within China but also militant organizations outside of China as long as their communications pass through places of Chinese-controlled infrastructure nodes. This practice makes cyber policy a tool to expand security responsibilities in crossing geography in accordance with expanded defense needs to deal with asymmetric warfare. The integration can, also, be seen in the prioritization of the sources of R&D funding, implemented in terms of central plans, according to which the scientific innovation agendas are directly linked to the military preparedness goals. Projects focus on the development of capabilities that would be applicable in both civilian economic competitiveness and defense systems: high-data encryption will provide secure trading and at the same time enhance classified military communications; high-resolution satellite imagery will aid in urban planning and at the same time, the quantum key distribution will provide unbreakable channels of data transmission to both government ministries and naval command fleets. By making it multipurpose technology development, it minimizes the difference between peacetime infrastructure development and the preparation of national security, it incorporates deterrence capability in the future within the current economic processes. More importantly, the integration is strengthened by the membership in the international norm-setting structures where China promotes the encryption standards and the routing guidelines that do not conflict with the local surveillance capabilities (Сюаньца & Гуаня, 2024, p. 3). An international adoption of such standards would harmonies the Chinese operational preferences of overseas digital environments, and would extend its defensive philosophy to overseas markets, without directly imposing constraint conditions on competitors whose system designs were not designed to be compatible with the Chinese. Diplomatic action in this case supports defense interests by providing normative authority over the control mechanisms that are the center of national cyber strategy, such that any future conflict is fought on technically favorable ground attained in advance as a result of governance influence campaigns. In the view of Pakistan, in witnessing these integrations, China exhibits a paradigm, where cyber strategy cannot exist outside of overall defence policy: technological independence serves as strategic hedge; legislation serves as legal fortification; foreign infrastructure initiatives establish long boundaries doubling economical roles and with latent protection measures; combined agency operations provide resilience to civilian infrastructure and military protection posture (Fatima & Maqbool, 2022, p. 6). The overall breadth puts smaller states in mind when opting selectively, full replication requires resource depth and political coordination that is hard to achieve outside the hegemonic circumstances, and provides an understanding of how priorities in the digital domain can make wider security policy without being seen as detached and apart of traditional power instruments.

Self-reliance Initiatives in Technology.

Efforts on technological self-reliance in China are components of a structural pillar of the cyber strategy that closely coincide with the strategy of industrial upgrading, economic policies, and geopolitical positioning. The overall goal is to minimize reliance on the overseas supply chain of both fundamental digital and semiconductor technologies and, at the same time, to have the capability equivalent or even higher than the international rivals. It is a strategy that is a direct reaction to perceived weaknesses which are increased through the pressure of outside forces like U.S. export block, investment limitations, and allied agreements that prevent China access to some of the high-performance components of computing. These limitations have resulted in Beijing to make self-reliance a national need and not desire, and entrenched it in civilian industrial planning on one hand, and military preparedness doctrine on the other. The semiconductor industry has been the key to these

efforts. The adoption of small yard and high wall-policies by the U.S. in limiting access to advanced lithography equipment by trilateral agreements with Japan and the Netherlands have highlighted the sense of urgency in regards to domestic substitution. Policy literature of China defines phases of development of low-end replacement parts to high-end research and development jumps with a focus on aligning design and national production capacity. The existing gaps are discrepancies between advanced chip designs created on local level and production facilities that can create them with competitive scale and relying on imported high-performance processors in industries like artificial intelligence (AI), aerospace, and secure communications. The industrial upgrading plans combine the enterprise-centered innovation and government-centered funding. The interrelation between the state direction, the educational research organizations and the corporate R&D units are guided by the model of new national systems which initially focuses on the concentration of resources in strategic categories (Jin, 2024, p. 8). In this model, the university laboratories team up with semiconductor makers to meet deep technical problems, like the control of etching to less than 10nm, as enterprise leaders develop solutions to package to Chinese hardware ecosystems. Co-ordination is also enabled by the use of state-subsidized industrial clusters to cluster the networks of suppliers, technological skills and specialized labour forces in strategic areas. Self-reliance is not limited to hardware, but software ecosystem, where the use of foreign proprietary codebase is being incrementally supplanted by home-grown codebase. Efforts in this are to work on operating systems, encryption suites, industrial control software and middleware frameworks that are significant to platform interoperability. Through the creation of compatibility between local systems and security measures that satisfy the national demands, China minimizes the exposure to internal weaknesses or the intentional downgrade of the products by third parties. This also allows greater localization of sensitive data storage, which is a staple of cyber sovereignty agenda identified above. Aerospace in an aerospace perspective, self-reliance in the avionics, aero engines, satellite navigation system (e.g., BeiDou), and hypersonic weapon guidance, are all combined with the development of cyber infrastructure. Aligning R and D on these regions with the indigenous semiconductor manufacturing as well as secure communications protocols, China is increasing its capacity to run advanced platforms without relying on overseas suppliers. This kind of integration is a wider awareness that technological independence in the cyberspace must be interoperable with other strategic sectors; dependence on foreign elements in military aviation or space systems might pose exploitable cyber weakness during emergencies. The emphasis on standard-setting as the aspect of self-reliance is further supported by international competition. Such engagement on technical committees is to harmonise global standards in relation to specifications that are favourable to domestically designed designs (Du, 2023, p. 9). This two-sided initiative has both foreign adoption and home interoperability, a Chinese-generated encryption algorithm or routing protocol can gain great acceptance in foreign markets, and thus enhance the competitiveness of the domestic industry, but it will decrease the dependence on foreign controlled standards organizations. Geopolitical factors involve expecting not just the disruption of supply chains due to sanctions, but also the unstable market conditions due to trade wars or instability in a region (Jin, 2024, p. 8). The exposure to the volatility of access to raw materials such as rare earth elements are inputs in the policies that drive vertical integration between mining activities, material refining facilities and final product assembly lines inside of China. This guarantees base materials all the way to top technologies continuously produce. One of the secondary dimensions is the talent nurturing. Understanding that the lack of human capital may halt technological autonomy despite the provision of the material necessities, Beijing is making significant investments into the STEM education pipelines of microelectronics, cybersecurity engineering, AI algorithm development, and applied physics that are applicable in the production of chips (Du, 2023, p. 9). Military schools in cooperation with non-military universities produces dual trained specialists who can be employed in the defense applications and commercial

innovation industries. This kind of cross-domain skill will be critical in maintaining long-term competitiveness as a result of the convergence between the civilian technology market and military cyber needs. Organizational wise such initiatives demand tradeoffs between shorter term substitution objectives over the long term innovation leadership objectives. China in the short run brings in technologies as the intermediary to ensure continuity of operations as it works on the development of replacements locally; in the long run China aims at export competitiveness by unique innovations other than through imitation. It is necessary to get this track by implementing coordinated efforts in fabrication precision engineering, proprietary intellectual property protection mechanisms based on domestic legal provisions of Section 4.2.2, and placement of market strategy Chinese products as viable alternatives that can be used in geopolitical headwinds across the world. To states such as Pakistan that are following these trends, the China road map may present a possible partner with whom to join in research and development, R&D ventures would speed up the development of the technology base in Islamabad and the procurement patterns would be aligned to interoperable platform in line with the governance sovereignty models. But with this cooperation, there are dependencies hidden, which means that once Chinese standards on top of supply lines are adopted, then future diversification will be constrained as interoperability barriers associated with political affiliation can be imposed by the rival blocs. The strategic autonomy implications highlight a point in the fact that technological self-reliance is not merely a matter of internal capability but includes the diplomatic adaptability in the competitive multipolar technology environments. These efforts eventually manifest a process of iteration, which is responsive to outside containment conditions but based on proactive structural transformation: replacing imports where possible; developing domestic design-to-production ecosystems; internalizing the principles of sovereignty into technical architecture; aligning cross-domain strategic requirements; affecting the world of global standards through engagement of standardizing operations; creating resource logistics all the way to base materials; developing an interdisciplinary pool of talents; and balancing replication by original innovation (Jin, 2024, p. 8). All the factors accumulate to minimize system vulnerability in cyberspace and increase the power of China in the greater geopolitical contesting with technological supremacy.

Domains of Competition

Economic and Industrial Espionage.

Through this economic and industrial espionage in Sino-U.S. cyber competition is both a tool of statecraft tactic and a tool of long-term benefit. The practice encompasses illegal obtaining of proprietary technologies, trade secrets, or commercially sensitive information that can change competitive equations in major sectors, particularly those that have a dual-use capability in which the civilian use is overlaid with the needs of the national defense (Du, 2023, p. 5). These activities are in most instances incorporated in larger national plans that combine the economic growth objectives with military-modernization needs and increasingly blur the boundaries between business innovation and maturation of security capabilities. In the eyes of Washington, the economic espionage operations by the Chinese have focused on the high-value segment of economic activities such as aerospace, electronics production, pharmaceuticals, and high-technology materials. The convergence can be exemplified by well-documented attacks into contractor systems associated with defense-related projects: stealing design files of stealth fighters or submarine technologies does not only weaken the corporate competitiveness but also speeds up the military programs of adversaries without comparable costs on investments into research and development (Zhou, 2023, p. 8). This is hardly opportunistic acquisition but is consistent with the articulated industrial policies like the Made in China 2025 that focus on command in key areas of technology. The realist perspective of these intrusions by U.S. security agencies is that they are attempts to seal the capability gaps, and avoid the high initial cost of local development. The official documents of Beijing often dismiss the claims

about Chinese-supported theft, referring to its technological success as the result of valid cooperation and foreign direct investment into joint-stock companies and home-based innovations (Zhou, 2023, p. 9).

However, secret evaluations in the Western intelligence circles indicate that China is using a multi-tiered system of operation; state-managed teams coordinate strategic infiltration into companies in other countries; quasi-autonomous actors, such as subcontracted research centers, glean intermediary data on a national level; and personal businesses may find value in stolen information through informal channels. Such distributed ecosystem makes it harder to do attribution work as it clouds overt command-and-control evidence whilst keeping nearly operational compliance with national objective. This complexity is manifested in operational techniques. Cyber-enabled espionage usually starts with reconnaissance to map target network architecture and find vulnerable endpoints, including poorly secured IoT devices as a part of manufacturing processes and insecurely patched enterprise software processing logistics (Du, 2023, p. 4). Phishing is one of the main entry vectors: hackers create emails imitating the correspondence of partners or the official regulatory messages in the industry where the target works. After access is gained, privilege escalation can be used to install customized malware that is used to ensure long-term persistence. The implants are not aimed at having incremental datasets infiltrated in large volumes over long durations rather than in large, one time thefts, being a method to prevent the operation of anomaly detection systems based on abrupt spikes of traffic. Supply chain infiltration is also used in industrial espionage. Through the introduction of malicious code or modification of hardware during the production phases (specifically, when the components are produced offshore), the actors can subsequently trigger defaulted functions that allow them to gather hidden data or modify the activities (Zhou, 2023, p. 8). Interestingly, these strategies have two purposes; they can be used to acquire intellectual property of a particular company and may also create a set of latent control systems that can be used during geopolitical emergencies against the whole segments of the industry. On the U.S. side, it is possible to countermeasures with the use of both technological hardening and legal prosecution approaches. Not only punitive but also used as a warning signal, indictments of named PLA officers of alleged cyber theft have been applied to underscore the risks to the individuals acting under official instructions (Zhou, 2023, p. 9). At the same time, export restrictions to crucial manufacturing equipment, including state-of-the-art semiconductor lithography machines, are meant to limit Chinese capacity to utilize stolen design to the fullest extent by limiting their production capacity.

Beijing self-reliance efforts are, however, aimed at counteracting these limitations by increasing the domestic fabrication capacity by creating focal points of investment and fastening training programs in specialization of technical jobs. The extent of economic spying is not solely on direct bilateral rivalry. When domestic firms in the third-party states possess technology applicable in either sectors of strategic interests, the states become incidental arenas. The inclusion of Pakistan in the projects such as CPEC has already attracted the attention of cyber actors to obtain engineering designs of transport infrastructure or energy grid designs (Khan and Bukhari, 2024, p. 4). Although they might appear out of bounds to the conventional high-tech rivalry, they are constituents of operational foundations that drive resource mobility and industrial durability that can indirectly affect global marketplace competitive findings. Industrial espionage has effect on normative discourses in the international forums focused on cybersecurity governance (Zhou, 2023, p. 8). The differences in definitions, as to whether this or that activity is legitimate competitor intelligence collection or criminal theft, continue to extend any effort to establish binding principles against targeting civilian commercial sectors. China is known to push norms of sovereignty where there are large margins of flexibility in controlling information flows within the country; the US advances transparency-based models based on protecting intellectual property across nations without regard to the host-state style of governance. These ideological differences do not allow an agreement regarding verification

mechanisms that will enforce prohibitions against economic espionage. Financial impacts are felt across economies that are impacted by the theft of an IP portfolio, beyond the direct loss value of the theft that is pinned on proposed IP portfolios. Accelerated rival replication competitive disadvantage leads to market share loss at a higher rate than incremental innovation cycles can restore, reduced levels of revenue restrict the ability to reinvest in future R&D, competition losses undermine trust eroding among investors, which makes capital costs higher, and the costs of insurance coverages are enhanced as coverage against cyber-related losses becomes more expensive under the repeated breach conditions (Du, 2023, p. 5). Supply Chain disruptions are also experienced when the manufacturers of high-value components observe the copies of their designs in another country and consequently the original partners diversify their sourcing to minimize the efficiency achieved by the long relationship developed between the supplier and the original partner. Geopolitically speaking, effective industrial espionage reacts to the bargaining patterns of trade negotiations by lowering the reliance on imported technologies or by enhancing the bargaining forces through the diversification of the product lines with global competitiveness. To the case of Beijing, the incorporation of misappropriated technological knowledge into its local production enhances its bargaining power in WTO negotiations or in bilateral trade agreements pertaining to the sector; to Washington, the exclusionary of such incorporation is an economic protection as well as an action that is strategic to restrict the potential dual use menace of exported Chinese machinery. The situation in Pakistan is quite delicate: balancing the requirements of infrastructure protection provided by China with the demands of cybersecurity defense and the demands of the US to protect personal information against technology leakage puts a strain on the harmonization of domestic policies (Khan and Bukhari, 2024, p. 4). The introduction of inspection regimes of imported hardware/software and not to lose the suppliers will have to be carefully balanced, especially as allied commitments involve confidentiality clauses that will not allow outside audits. Lack of control over this balance means there could be some vulnerabilities that can be manipulated by actors who use political shift of alignment or compliance loopholes in the industry. Overall, economic and industrial espionage is the business and strategic meeting point in Sino-U.S. cyber competitiveness, which is an ongoing competition associated with integrity of the supply chain, market dynamics, normative legal framework, loyalty tests within an alliance, and indirect exposures to third-party states caught between competing operational philosophies (Zhou, 2023, p. 9). Its strength as a tool of diplomatic mitigation is that it is useful: the acceleration of capability development by using the covert acquisition method requires no proportional increase in resources used to obtain it and the plausible deniability of non-escalation to open conflict avenues.

Cyber space applications in the military.

Cyberspace uses in the military are a threshold in itself, in strategic confrontation, a capability enabler, as well as a multiplier of effects in all arenas of operation. Cyber tools are applicable in various functions of contemporary force structures: they can degrade the enemy systems, defend own infrastructures, carry out pre-emptive intelligence collection, and influence the battlefield conditions by manipulating command-and-control nets. The discourse employed by the U.S. Department of Defense and the Chinese People's Liberation Army (PLA) is similar to their perceived notion at the inseparability of the cyber sphere and traditional power projection, but they are different in their doctrinal views, organizational integration, and focus on operations (Sari, 2019, p. 12). On the offensive front, cyber operations are planned as parts of the larger military operations to deliver the same effects as the kinetic attack but without the physical destruction. This involves shutting down enemy radar grids through malware injections, sabotaging logistics databases and messing with deployment resupply chains, or compromising satellite links at critical deployment periods (Katkova & Yunyushkina, 2022, p. 3). PLA doctrine considers Computer Network Attack (CNA) a premium means of achieving the so-called soft kill, in which systems are not destroyed, but made effectively

useless, thereby enabling psychological pressure at the same time, by diminishing perceived technological reliability in an enemy force. Likewise, U.S. strategies spell out the concepts of persistent engagement under the authority of USCYBERCOM to work in adversary networks prior to the escalation of conflict, and thus limiting their ability to organize well in case of escalation (Du, 2023, p. 8). Military readiness is no less mixed with defensive applications. Some of the measures taken by cyber defense include ensuring that weapons systems cannot be exploited during their service maintenance, making embedded firmware in missile guidance units' resistant to unauthorized reprogramming and safeguarding classified channels of communication between dispersed units. The tasks have been highlighted by the planners of PLA as part of Computer Network Defense (CND) where resilience is considered vital in maintaining deterrence credibility (Katkova and Yunyushkina, 2022, p. 9). The U.S. uses its philosophy of defend forward in order to move defense into enemy digital space to preempt threats before it can affect military assets in the country (Du, 2023, p. 8). Intelligence enabled by cyber adds more range to military application. Computer Network Exploitation (CNE) enables non-destructive reconnaissance within enemy networks: mapping the topology of defensive mechanisms; locating high-value nodes on which subsequent CNA attacks will be launched; and scavenging strategic planning documents or materials used in weapons systems (Сюаньцзя & Гуania, 2024, p. 3). CNE can facilitate the industrial espionage of defense contractors overseas in the context of PLA usage, as detailed in Section 4.3.1, directly into the pipeline of local R&D. CNE is used by the U.S. forces to perfect targeting matrices to special operations and inform diplomatic positioning by exposing operational patterns of the opposing forces. It is especially integrated with other fields in space and electronic warfare. Attacks on cyber space against satellite control networks are able to modify the imagery streams or navigation data e.g. redirecting GPS data or corrupting BeiDou outputs to disrupt maneuver precision and coordination. These trickle quickly into land, air, and naval theatres where precision depends on a continuous flow of data supply of orbital assets. Considering these disruptions as a possible force multiplier, both China and the U.S. believe this may undermine enemy situational awareness without necessarily going to armed conflict against an enemy to destabilize tactical balances during a crisis. Military cyber strategy is a wide overlap of information warfare. The PLA includes psychological operations, spreading fake orders or fake reports via compromised channels, as a part of a concept of integrated network-electronic-psychological attack (Katkova and Yunyushkina, 2022, p. 9). These type of strategies undermine morale and cause confusion among command along with the chain of command even before any kinetic action is taken. Although the U.S. is also actively involved in its activities of information shaping through the use of cyber, it is oriented toward integrating the influence campaigns with specific CNA activities aimed at undermining the trust in the leadership decisions under the conditions of a real time pressure (Du, 2023, p. 8). The following dynamics can be illustrated by operational examples: manipulation of transportation management systems as simulated delays in the efforts of the adversary forces to deploy their forces; the introduction of malicious code into automated maintenance scheduling systems of aircraft and subsequent unexpected grounding; the creation of false sensor warnings in order to redirect defensive resources to non-targets of actual infiltration (Katkova and Yunyushkina, 2022, p. 3). These situations point to the asymmetrical advantage of cyber operations combined with their cost-effectiveness compared to kinetic solutions combined with the ability to deliver strategically decisive effects when timed right. Another dimension lies in the overseas aspect: cyber infrastructures installed through ICT projects by foreign companies will now be a dual-use element in conflict paradigms (Sari, 2019, p. 3). The Chinese-created port management software on Belt and Road routes might theoretically be re-purposed to track the movements of the navy; or port access control allocation during a crisis; American-supplied secure communication hardware in allied forces could also be used as integration hubs to allow rapid response in crisis regions. Pakistan, in its turn, experiences exposure in both dependencies on

imported defense technologies, which may have exploitable backdoors, and in belonging to regional alliances, in which cyber interoperability needs may conflict operations networks with the architecture of one of the major power at the cost of flexibility (Du, 2023, p. 8). As an illustration, the use of Chinese secure regimes in common exercises enhances trust, but may make interoperability with U.S.-supported allies difficult because of incompatible encryption regulations, a strain entrenched in the military applications of cyberspace. The overlap of cyber capability and conventional force employment implies that the risk of disruption is not confined to the battlefield; industrial bases that provide materiel can be crippled by organized CNA attacks; recruitment pipelines and popular support can be manipulated by coordinated information operation utilizing social media algorithms; even training programs may be compromised in case of the use of malicious updates to the simulation platform. Finally, applications of cyberspace to the military demonstrate the reason why competition remains fierce: dominance over this space generates opportunities to gain an advantage without an equivalent amount of resources spent on building traditional setups; it allows exerting control over the functioning across all arenas while maintaining deniability in cases of attribution challenges; and it is an ability to influence the processes before a hostile conflict leads to an open fight (Du, 2023, p. 8; Katkova and Yunyushkina, 2022, p. 9; Sari, 20

Political Influence and Information Operations.

The Sino-U.S. cyber rivalry largely involves political influence and information operations that are used to achieve goals that could avoid direct kinetic action and still affect policy decisions and the general attitude of the opponent. These operations, in most ways, are a complement to those in the military described in Section 4.3.2, but they also spill over to the civilian and diplomatic realms in which the ability to control the narratives can shift the cohesion of the alliances, the legitimacy of the domestic regime, and the direction of the policy-making without necessarily deploying conventional forces. In the case of China, Chinese political influence campaigns have frequently been through greater goals of cyber sovereignty. Being able to dominate local informational landscapes, Beijing protects its people against the narratives that could be viewed as destabilizing or threatening to party legitimacy (Mokry, 2024, p. 3). They are mechanisms of regulatory gatekeeping of online space, incessant surveillance of foreign-agenda-related content and specifically targeting suppression of politically sensitive information. It is these domestic actions that enable the state to offer a unified account back home to promote its larger strategic goals, be it the portrayal of Western criticism as hypocrisy, the presentation of trade conflicts in a way that is more likely to be favored by the audiences of China, or the rebranding of the tensions in the region through a language that focuses on peaceful building under the leadership of China. The influence operations that are externally oriented use not only open platforms, which are state media outlets with an international audience, but also secretive digital actions using coordinated social media activity in networks of pseudonymous accounts (Mirza & Akram, 2022, p. 13). The latter may push pro-China propaganda or create doubt about the intentions of the enemies, which is often amplified by automated bots or content farms to feel a consensus. These methods are becoming intertwined in disinformation where they would only focus on providing facts selectively or bend the facts to undermine competitor credibility. This strategy is a variation of the psychological warfare in PLA doctrine where manipulation of perception of the enemy is as useful as attack on the technical apparatus (Hjortdal, 2011, p. 8). In the viewpoint of the U.S., the information operations in the cyber space consists of defensive counter-narratives to highlight foreign propaganda campaigns as well as offensive influence to enlist coalitions against perceived threats by Chinese activities. Naming and shaming certain Chinese actors in cyber incidents are purposeful in this context, as they convey that it is possible to detect and respond to such incidents and frame China in negative terms with its friends (Mirza and Akram, 2022, p. 15). Coupled with the release of intelligence via diplomatic information or partners in the media ecosystem, these messages reinforce the will of the partners in common who

are concerned about the security posture of Beijing in terms of cyber-related matters. Timing is important; attributing statements to release them at politically sensitive times or military operations can create a bias by causing you to put less faith in counterparts by confusing them with those situations. Both parties mobilize the use of the multilateral forums in political signaling in the cyber discourse. China implements mechanisms such as ASEAN Regional Forum to sell the sovereignty-based control models in the name of stability advocacy (Zhou, 2023, p. 9), implicitly urging states in the region to embrace the principles of governance that are consistent with its home regulatory system. The U.S., in its turn, promotes multi-stakeholder practices and open-network principles (Zhou, 2023, p. 2) and entrenches these preferences in capacity-building programs that are based on cooperation and do not require stringent regulatory requirements to states willing to receive technological support. The models have political messages, which aim at luring sympathetic states into respective spheres of influence. The Economic interests also interface with the information operations. The campaigns of alleged misbehavior of the foreign companies doing business in China or vice versa are planned to be launched at the appropriate moment, either during the negotiation of the trade agreements or during the hearing of the regulations (Du, 2023, p. 5).

The direct impact of these narratives on market pressure can occur without any formal policy actions since they can alter the opinion of the masses to support the champions of national industry or distrust the products of competitors. Non-state actors are an instrument to broader influence policies in hybrid situations involving cyber terrorism and political propaganda. The surveillance of terrorist groups that rely on social media to recruit or spread their messages is the prime target in case of infiltration to disrupt or redirect such communication by the major power intelligence organizations (Mirza & Akram, 2022, p. 13). The discourses of these channels can be manipulated by the states to construct narratives of competence and moral authority in counterterrorism, such as in cases where the operations are mediated digitally and not interdictions. Attribution problems make it difficult to respond to influence operations as is the case in technical attacks. The covert operations are organized in such a way that they can be denied; the lines of command between the state officials and the actual executors are covered by numerous layers of intermediaries (Hjortdal, 2011, p. 10). This allows a permanent campaign action that does not result in diplomatic explosives. As a case in point, when the sources of inflammatory material are accounts with indirect connections in foreign jurisdictions through complicated ownership arrangements, responsibility becomes hard to trace so that competitors need to assess the cost-benefit analysis of determining whether to make official accusations. In the Pakistani experience of stumbling in these kinds of interactions, both the Chinese and the U.S. campaigns of political influence confer real consequences on domestic conversations regarding the use of technology, commitment to alliances, and posture towards regional security. Messaging integrated into the cooperative projects, be it the capacity-building events related to U.S.-linked institutions or the infrastructural development of the projects funded by Chinese money, can influence the opinion of the elite in a way that makes them focus more on fitting into one of their camps (Sari, 2019, p. 12). Similarly, focused accounts that contextualize Pakistan as technologically vulnerable or that present some of the procurement decisions as strategically risky can be felt in policymaking to the extent that they are externally created. The information campaign toolkit incorporates the use of simulated grassroots campaigns via online communities (so-called astroturfing), amplification of positive discourses through search engine optimization on the basis of multilingual content pools, and capitalization on trending topics on social media sites in case of a crisis situation. The networks using PLA links have proven the ability to quickly switch thematic attention basing on geopolitical signals; like U.S. aligned actors will use dynamic targeting models that are founded on the output of sentiment analysis by AI-led surveillance networks (Hjortdal, 2011, p. 8).

Conclusion

The USA-Sino cyber rivalry had a deep impact on the global politics and both countries want to control and hegemony in the arena of international politics. Both nations are giving prime importance to the matter and considered it as vital tools for the national security, Ideological influences and for the Economic Advantages. This rivalry encompasses the cyber espionage, the development of the offensive and defensive infrastructures and also for the intellectual property theft.

References

Ahmad, S. (2022). CYBER SECURITY THREAT AND PAKISTAN's PREPAREDNESS: AN ANALYSIS OF NATIONAL CYBER SECURITY POLICY 2021. Pakistan Journal of Humanities & Social Sciences Research, 5(1). https://doi.org/10.37605/pjhssr.v5i1.381

Akram, N., & Tariq, K. (2024). War on terrorism in pakistan: Security challenges and safety prioritization. Social Science and Humanities Journal, 08(04), 34765–34782. https://doi.org/10.18535/sshj.v8i04.981

Alatas, S. F., & Ushama, T. (2023). Intellectual discourse (1; Vol. 31). https://journals.iium.edu.my/intdiscourse/index.php/id

Bhatti, G.-A. Great power rivalry in the indian ocean and its impact on pakistan. Journal of Nautical Eye & Strategic Studies, 113.

Chan, A. (2013). The resistance of walmart workers in china: A missed opportunity.

Chen, J. (2022). The new evolution of china's diplomacy with arab states under the background of the sino-u.s. Competition: Trends and prospects. Chin Arab Stu, 2(2), 173–185. https://doi.org/10.1515/caas-2022-2015

Du, G. (2023). The role of high-end manufacturing in sino US trade friction. BCP Business & Management EMFRM, 38, 3184.

Fatima, N., & Maqbool, T. (2022). US - INDO PACIFIC STRATEGY AND ITS IMPLICATIONS ON PAKISTAN. Pak. Journal of Int'L Affairs, 5(3), 38.

Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. Journal of Strategic Security, 4(2), 1–24. https://doi.org/10.5038/1944-0472.4.2.1

Hughes, C. W., & Kallender, P. (2016). Japan's emerging trajectory as a 'cyber - power' : From securitization to militarization. Journal of Strategic Studies, 40(1–2), 118–145. https://doi.org/10.1080/01402390.2016.1233493

Imran, S. Sino -US involvement in afghanistan : Implications for south asian stability and security.

Jin, Z. (2024). Thinking inertia and path dependence in US chip hegemony strategy. Transactions on Economics, Business and Management Research, 7.

Katkova, E. Yu., & Yunyushkina, A. S. (2022). Chinese concepts and opportunities in information warfare: China–US rivalry in cyberspace. RUDN Journal of World History, 14(2), 197–210. https://doi.org/10.22363/2312-8127-2022-14-2-197-210

Khan, M. N. A., & Bukhari, S. M. H. (2024). The sino-pak strategic partnership and india's regional aim in south asia: An analysis. Journal of Social Sciences Development, 3(2), 81–92. https://doi.org/10.53664/JSSD/03-02-2024-07-81-92

Li, A., & Chen, Y. (2017). Research on sino - US cybersecurity law enforce ment cooperation from the perspective of international law enforcement cooperation. In Advances in Social Science, Education and Humanities Research (Vol. 124, p. 1058).

Liu, C. (2023). Reconstruction of sino–US relations and deepening ASEAN relations in the post epidemic era. International Journal of Education and Humanities, 10(1), 131.

Mirza, M. N., & Akram, M. S. (2022). 3-cs of cyberspace and pakistan: Cyber crime, cyber terrorism and cyber warfare. Strategic Studies, 42(1), 62–80. https://doi.org/10.53532/ss.042.01.00134

Mokry, S. (2024). Grand strategy and the construction of the national interest: The underpinnings of sino–US strategic competition. International Politics, 61(1234567890), 742–760. https://doi.org/10.1057/s41311-023-00452-w

Pasaribu, R. S., Muchaddats, M. F., & T. R., D. (2024). RANCANGAN RECEIVER ADS -b MENGGUNAKAN RTL -SDR UNTUK PEMBACAAN DATA ASTERIX DI PROGRAM STUDI TEKNIK NAVIGASI UDARA. Jurnal TNI Angkatan Udara, 3(2).

Priya, & Singh, K. (2024). Emerging cyber security and data privacy threats: Challenges and opportunities: An analytical overview. International Journal for Multidisciplinary Research (IJFMR), 6(2), 1. www.ijfmr.com

Pugliese, G., Fischetti, A., & Torri, M. (2022). US-china competition, COVID-19 and democratic backsliding in asia. In ASIA MAIOR (2).

S, G. P. B., M, Dr. K. G., & HA, Dr. D. (2023). AI-driven cyber security: Security intelligence modelling. International Journal of Multidisciplinary Research and Growth Evaluation, 04(06), 961–965. https://doi.org/10.54660/.IJMRGE.2023.4.6.961-965

Sari, B. (2019). Making sense of the new episode of great power rivalry in africa through neorealist lenses: The sino-US competition. Journal of Global Studies, 4(4). https://doi.org/10.20889/M47e20014

Sarker, K., Rahman, H., Rahman, K. F., Arman, Md. S., Biswas, S., & Bhuiyan, T. (2019). A comparative analysis of the cyber security strategy of bangladesh. International Journal on Cybernetics & Informatics (IJCI), 8(2), 1. https://doi.org/10.5121/ijci.2019.8201

Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. Chinese Political Science Review, 1, 81–93. https://doi.org/10.1007/s41111-016-0002-6

Smith, N. R., & Brown, R. J. (2021). Neither a new cold war nor a new peloponnesian war: The emerging cyber-narrative competition at the heart of sino-american relations. Vestnik RUDN. International Relations, 21(2), 252–264. https://doi.org/10.22363/2313-0660-2021-21-2-252-264

Sun, W. (2023). Research on the extraterritorial application of china's antitrust laws in the context of the sino-US trade war. International Journal of Frontiers in Sociology, 5(13), 46–51. https://doi.org/10.25236/IJFS.2023.051309

Syed, F. Z., & Javed, S. (2017). Deterrence: A security strategy against non traditional security threats to pakistan. Int. J. Soc. Sc. Manage., 4(4), 267–274. https://doi.org/10.3126/ijssm.v4i4.18503

Tehseen, M. Sino -US competition: Implications for south asia and the asia -pacific.

Vinhas de Souza, O. (2024). Russia's invasion of ukraine and national cyber security strategies: Quantitative comparison. Acig, 3(1). https://doi.org/10.60097/ACIG/190346

Wu, Y. (2024). The combination of hedging and rules of great power rivalry–taking the example of vietnam in sino–US rivalry. Highlights in Business, Economics and Management WTED, 35, 8.

Yuen, S. (2015). Friend or foe? China Perspectives, 3, 51–56. https://doi.org/10.4000/chinaperspectives.6807

Zhou, B. (2023). A cognitive discourse study of the US's cognition of china in sino-american strategic competition. Studies in Asian Social Science, 9(1), 1. https://doi.org/10.5430/sass.v9n1p1

Селянин, Я. В. (2023). Противостояние США китаю через призму киберпространства. Россия и Америка в XXI Веке, 2023(3). https://doi.org/10.18254/S207054760026344-5

Сюаньцзя, Л., & Гуаня, С. (2024). Цифровая гегемония США: Особенности, цели и последствия. Государственное и Муниципальное Управление. Ученые Записки, 2, 297–301. https://doi.org/10.22394/2079-1690-2024-1-2-297-301

Федоров, Н. В., & Гарин, А. А. (2023). Оборонное и экономическое сотрудничество индии и вьетнама в увязке с проблематикой южно -китайского моря. Вьетнамские Исследования, 7(1), 5–16. https://doi.org/10.54631/VS.2023.71-111035