ARTICLE

The U.S.-China Cyber Warfare in the 21st Century: Implications for International Security

SARMAD ALI KHAN* **and SAIRA NAWAZ ABBASI****

* Bahria University, Pakistan
ORCID No: 0000-0002-5165-8123

** Bahria University, Pakistan
ORCID No: 0009-0001-4598-1311

ABSTRACT *The power competition between the major powers of the world has always been dependent on the strategic security landscape. Over the years, military operations and warfare have evolved with the development of new weapons, equipment, and technologies. During the 20th century, the world witnessed a transformation from conventional strategic competition to unconventional strategic competition with the advent of nuclear weapons. The genesis of the 21st century marked another revolution in military affairs when electronic warfare was modernized and cyber warfare came into the spotlight. In the current century, new poles of powers have emerged whereby Beijing and Washington started competing at all levels and in all domains. Shortly after the incorporation of digital, electronic, and cyber equipment and techniques by militaries around the world, cyberspace became militarized and emerged as the fifth battlefield. The U.S. armed forces and the Chinese PLA both rely heavily on cyberspace when it comes to their communication, operations, and planning. Cyber campaigns launched by Washington and Beijing on various targets accounted for a cyber arms race and continuous cyberspace strategic competition between the two countries.*

Keywords: Cyberwarfare, USCYBERCOM, International Security, Military Operations, PLA, General Staff Department

Insight Turkey 2023
Vol. 25 / No. 2 / pp. 163-185

Received Date: 2/8/2022 • **Accepted Date:** 12/4/2023 • **DOI:** 10.25253/99.2023252.10

China-U.S. Strategic Competition in the Cyber Domain

The strategic competition between Washington and Beijing continues to shape the international security environment and subsequently pull the strings of regional and sub-regional security structures in the 21st century. The contemporary global security landscape finds its roots in the traditional patterns of operations but is driven by non-traditional components of security. This is because the dawn of the 21st century coincided with technological revolutions that not only affected the international civil standard operating procedures but also revamped the approach of militaries. Being at the crossroads of conventional and unconventional aspects, cyberspace strategic competition between the United States (U.S.) and China also started in the last decade of the 20th century when the two countries neither confronted each other formally labeled cyberspace as a war-worthy domain. However, recognizing each other's cyberspace capabilities, as well as those of other countries, they started formalizing cyberspace warfare strategies and policy guidelines. It was in the early 2000s when China and the U.S. highlighted the shift in their military postures and doctrinal changes in which cyberspace emerged as a zone of competition along with other military domains. Initially, cyberspace capabilities were used by existing military structures as force multipliers and to support traditional military campaigns. As technology progressed and cyber warfare capabilities matured, cyber warfare capabilities evolved into independent and joint components for military operations. After both countries recognized cyberspace as the 5th warfighting domain, cyber warfare's importance enhanced multifold. With security situations around the world becoming more volatile, controlling the escalation ladder becoming difficult and complexities increasing day by day, cyber warfare became the ideal weapon of choice with many advantages such as anonymity, non-use of kinetic options, no confrontation, and so on. The establishment of dedicated cyber warfare wings, the development of cyber weapons, and the militarization of cyberspace by Beijing and Washington spurred a cyber arms race between the two countries as emerging superpowers. It also elicited the concept of a balance of power in cyberspace for either of the one to dominate and gain strategic cyber warfare leverage over the other.

U.S. Cyber Warfare Capabilities: Structures and Functions

Over the last three decades, the strategic posture of the U.S. has transformed vis-à-vis its security policies. The U.S. has actively developed and incorporated cutting-edge and disruptive technologies in its military doctrines and has also manifested them practically in various military operations. The American military has invested heavily in developing capabilities in the cy-

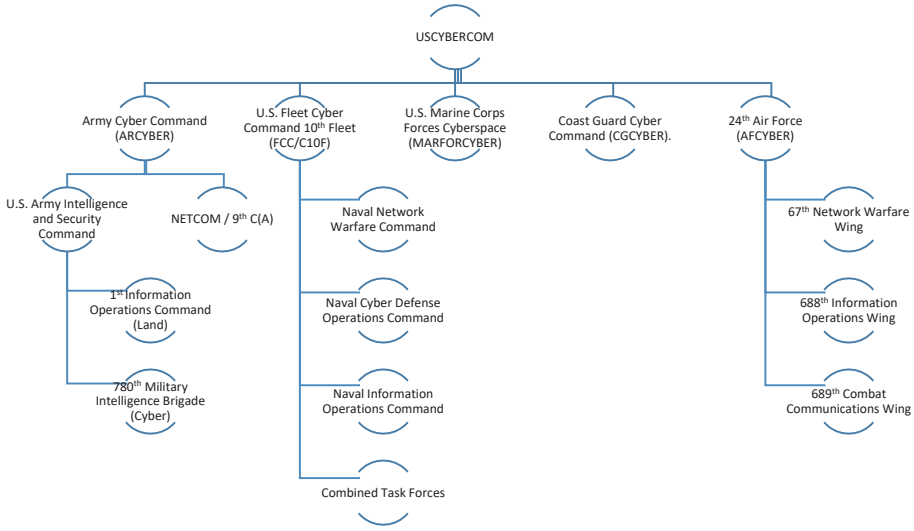
berspace domain, particularly to weaponized it. This, in turn, has led to spillover effects on conventional military capabilities and operations.[1] The establishment of the U.S. Cyber Command (USCYBERCOM) in 2009 highlighted the importance of cyber warfare for the country.[2] USCYBERCOM was initially tasked to "direct, synchronize and coordinate cyberspace planning and executions" for defending the U.S. and its national interests.[3] With its establishment, USCYBERCOM emerged as a capable component based on the co-development of the 'Stuxnet' worm with Israel to disable Iranian nuclear plant centrifuges.[4]

The establishment of dedicated cyber warfare wings, the development of cyber weapons, and the militarization of cyberspace by Beijing and Washington spurred a cyber arms race between the two countries as emerging superpowers

The increased reliance on and usage of cyberspace by the American military enhanced the scope of operations for USCYBERCOM. Within a decade, USCYBERCOM evolved into a "unified combatant command" in 2018. Prior to this, the U.S. Strategic Command (USSTRATCOM) regulated USCYBERCOM.[5] The upgradation of USCYBERCOM into a distinct combatant command also resulted in the attachment of four service commands with it, namely the U.S. Fleet Cyber Command, the U.S. Army Cyber Command, the Marine Corps Forces Cyberspace Command, and the Air Force Cyberspace Command. The road map outlined by the U.S. Department of Defense (DOD) highlights that a cyber mission would be created for USCYBERCOM under which the command would maintain 6,200 personnel divided into 133 teams.[6] Moreover, these 133 teams are subdivided to conduct various tasks: 13 mission teams would defend against cyber threats; 68 teams are tasked with the cyber protection of the DOD's networks and systems against threats; 27 teams are combat mission teams designated "to conduct integrated cyberspace attacks" whereas 25 cyber support teams would provide back-end "analytic and planning support" to the aforementioned teams.[7]

Recognizing the relevance of cyberspace in a strategic context, the DOD publicized a report highlighting USCYBERCOM's road map. Complementing the 2018 U.S. National Defense Strategy, it outlined that USCYBERCOM must develop superiority over its adversaries as the armed forces have done in the physical domains. The role of American "cyber warriors" becomes crucial as some of the country's adversaries have become "near-peer competitors" and pose persistent threats to the U.S. economy and military.[8]

Figure 1: The Structure of the United States Cyber Command



Sources: *NATO Cooperative Cyber Defence Centre of Excellence and Security Affairs*[9]

U.S.' Multi-Faceted Cyber Warfare

Cyberspace has been recognized as a warfighting domain by the U.S. The widespread use of communications and technology has strategic threats attached to it and has accounted for the development of new techniques of coercion. Cyber warfare has become a "new normal" for adversaries to strategically compete with the U.S. For the U.S., cyber warfare is a multi-front strategic phenomenon with a trans-regional nature. According to the U.S. Cyber Command Vision, various states and non-state actors (NSAs) continue to launch cyber warfare or cyber campaigns against Washington to destabilize it economically and militarily.[10] The development of high-end military capabilities by its adversaries, including China, North Korea, Russia, and Iran, have reduced Washington's conventional military advantage and the aforementioned countries continue to compete in cyberspace on a strategic level. In addition, NSAs, including terrorists, hacktivists, etc., continue to exploit cyberspace against the U.S. Militant organizations like al-Qaeda, the Islamic State of Iraq and Syria (ISIS) and their affiliated groups have launched cyberattacks and cyber campaigns detrimental to American interests.[11]

The Indo-Pacific Strategy Report made public by the DOD in 2019 highlighted that Chinese military modernization and its subsequent military operations have an increased reliance on complex cyber warfare and electronic warfare.[12] Similarly, it highlighted the use of cyber warfare by North Korea to steal data for generating revenue. Taking into account these challenges, the U.S. plans to invest resources in conducting defensive and offensive cyberspace opera-

tions.[13] The multi-dimensional threats of cyber warfare against the U.S. are to be addressed through tailored strategies. Admiral Mike Rogers, a former commander of USCYBERCOM, prioritized five broad goals for the command that are as follows:[14]

The first country to develop disruptive technologies, particularly cyber warfare capabilities, in Asia, was China

i. Highly trained and ready cyber force,
ii. Creation of cyberspace situational awareness for the military,
iii. Development of operational concepts and command-and-control systems to execute missions,
iv. Establishment of joint and integrated defensible network,
v. Presence of competent authorities and the right policies to conduct full-spectrum operations in the domain.

As mentioned earlier, the role of USCYBERCOM snowballed after its inception from solely defending the country's military networks from the threats posed by cyber espionage to conducting cyber offensives and supporting joint military commands. Under the Trump Administration, the elevation of USCYBERCOM to a unified combatant command resulted in the transformation of its application trajectory as well. It was communicated by the U.S. Department of Defense that USCYBERCOM "is prepared to generate cyber effects" with decisive outcomes that demonstrate the rapid growth of the command.[15]

China's Cyber Warfare: Infrastructure and Applications

The first country to develop disruptive technologies, particularly cyber warfare capabilities, in Asia, was China. The strategic use of cyber warfare by the Chinese military started in the mid-1990s under the banner of the information warfare (IW) plan. By 1997, China had conducted multiple cyberspace exercises to interrupt, disrupt, and neutralize military communications.[16] In the same year, the Chinese Central Military Commission established a 100-member elite corps for an offensive role against the command and control systems of the U.S. and other Western countries. The 21st century increased the reliance of the Chinese military on cyber warfare capabilities and thus a strategic information warfare unit was formed. The unit's primary task was to engage with Chinese adversaries through computer networks for manipulating their fire control and guidance systems. American observers termed the IW unit as "Net Force."[17]

At the beginning of the 21st century, cyber warfare proved beneficial for the Chinese military as it supported asymmetric capabilities and simultaneously

In the contemporary strategic landscape, inter-state conflicts predominantly involve either proxy wars or unconventional warfare whereby cyber warfare becomes a potent tool for the militaries to employ against their respective adversaries

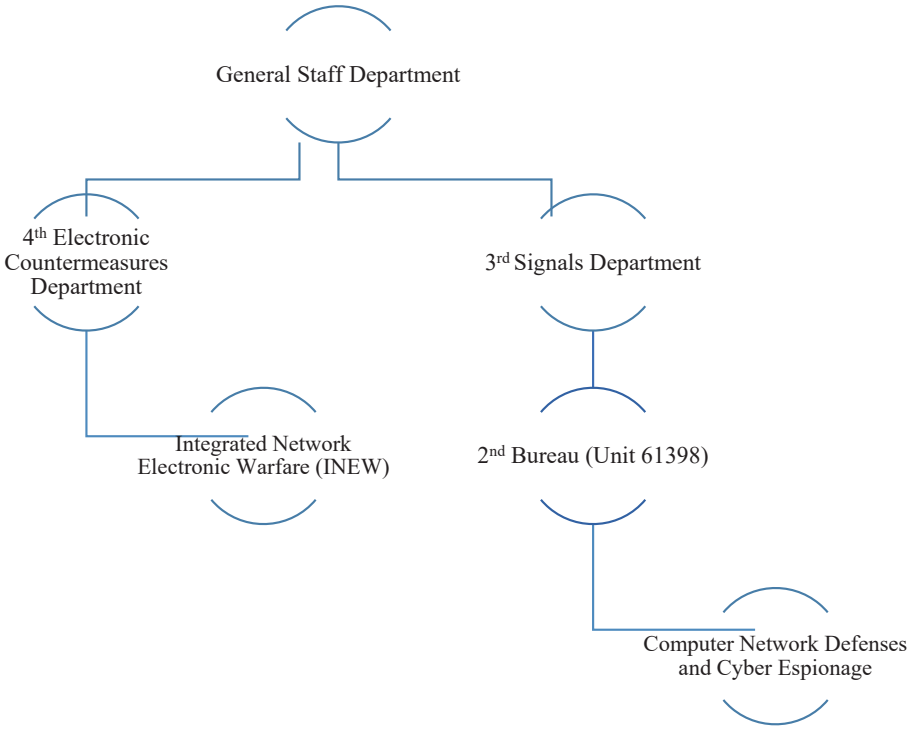
minimized the conventional disparity vis-à-vis the U.S.[18] The country also created an information-based all-inclusive master system to support its military operations by first giving rise to a joint[19] and then an integrated command and control system.[20] The People's Liberation Army (PLA) defines cyberspace as a domain "created by technology, computers, and the web."[21] The components of the domain are digital space, cyberspace, and information space, which are subject to continuous human intervention and control.

The year 2010 marked another important and crucial development when an "information protection base" was established under the General Staff Department (GSD) by the PLA. The base was given the task of security or defense of computer networks.[22] Chinese military's *White Paper*, published in 2014, recognized the importance of cyberspace for social and economic development and its integration with national security. It also called for the development of a robust cyber force with top-notch cyber warfare capabilities –both active and passive– along with international cyberspace cooperation to strengthen Beijing.[23] The importance of cyberspace for Beijing can be analyzed from the fact that in its 2019 *White Paper* named *China's National Defense in the New Era*, cyberspace is directly associated with the country's sovereignty and security interests.[24]

The organizational structure of Chinese cyber warfare is different from the American one. The computer and network attack missions are merged with the electronic warfare (EW) mission to form the "integrated network electronic warfare" (INEW) system. The INEW is regulated under the General Staff Department's (GSD) 4th Electronic Countermeasures Department. Moreover, the 3rd Signals Intelligence (SIGINT) Department controls computer network defenses and cyber espionage.[25] The General Staff Department's 3rd SIGINT Department monitors foreign communications, conducts cyber surveillance on high-priority targets, and protects the PLA's communication networks and computer systems. The Chinese SIGINT is the most sophisticated and comprehensive when it comes to the Asia-Pacific region. The 4th Department of the GSD has a portfolio of electronic intelligence (ELINT).

The cyber warfare organizational structure of the People's Liberation Army is shown in Figure 2 below:

Figure 2: The People's Liberation Army's Cyber Warfare Structure



Source: *Advanced Modernization and Preparation for War: Informatized Warfare, New Force Elements, Cyber, Space, Logistics*[26]

Training exercises for the INEW at the unit level involve computer network operations, spoofing, espionage, jamming, and components of electronic warfare. The cyber force working under the INEW is known as the Informationalized Blue Force. The Informationalized Blue Force was initially tasked to take hold of the enemy's (Red Force's) command and control system.[27] Chinese cyber operations have involved a wide range of targets such as command and control systems, supervisory control and data acquisition (SCADA) systems, logistic components, internet networks, and even weapons systems.[28]

Cyber Warfare as an Enabling Component for Militaries

The global strategic landscape has witnessed a substantial transformation in terms of technological induction in military theory, military planning, and military operations. The weaponization of cyberspace has highlighted its importance for militaries and NSAs and the scope of its application has proliferated subsequently. In the contemporary strategic landscape, inter-state conflicts predominantly involve either proxy wars or unconventional warfare whereby

U.S. Secretary of State Antony Blinken met with Chinese State Councilor and Foreign Minister Qin Gang in Beijing, to hold talks on many issues, including cyber security, June 18, 2023.

CHINESE MINISTRY OF FOREIGN AFFAIRS / AA

cyber warfare becomes a potent tool for the militaries to employ against their respective adversaries. Many international organizations and scholars equate viruses, harmful codes, etc. to weapons of mass destruction (WMDs), which account for the global cyber arms race. This also questions the applicability of non-proliferation treaties in the cyberspace domain.[29] Countries around the world have developed dedicated military-led cyber capabilities to increase their national power and achieve specific military outcomes.[30]

The significance of cyber warfare capabilities for militaries can also be gauged by former Chairman of the U.S. Joint Chiefs of Staff Gen. Martin E. Dempsey's statement in which he said, "We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse."[31] To connect this statement with the global security landscape, it is important to note that 20 countries (or more) have established dedicated military units to conduct cyber warfare.[32] Cyber warfare is not only detrimental to an adversary's military but can also handicap its economy, on which all the other elements of national power are dependent.[33] Hence, militaries can target a non-military target through operations in the cyberspace domain and achieve strategic results since the domain is not regulated like battlefields or war zones.

In modern warfare, all three levels of warfare rely directly on information operations (IOs) and network-centric operations (NCOs). From drafting doctrines to determining operational needs to planning and executing battles,

information, and network-centric operations dominate the cycle. Both of these operations are intertwined with cyberspace and associated capabilities. To integrate the tri-services operations and achieve a full-spectrum approach, integrated cyberspace capabilities are to be employed for enabling any military to influence, disrupt or deny the adversary's decision-making while protecting the owned systems.[34] Contemporary battlefields continue to draw primary support from computer networks and communication systems that operate modern and autonomous weapon systems. Cyber warfare enables militaries to penetrate the aforementioned systems, reprogram the data of these systems, and redirect a weapon to any other location for a strike. Similarly, through cyberattacks, the global positioning system (GPS) or command and control (C2) structures can be compromised, denying an adversary the ability to operate or even control its forces.[35]

Cyber warfare enables militaries to penetrate the aforementioned systems, reprogram the data of these systems, and redirect a weapon to any other location for a strike

Before the advent of nuclear weapons, the task of armed forces was to win wars but after the usage of nuclear bombs, the responsibility of militaries was to avert wars. The incorporation of cyber warfare fused with the notion of averting war resulted in intense competition in the domain of cyberspace. Unlike the conventional domains, warfare in cyberspace is relatively cheaper and below the threshold of an all-out war, which makes it a preferable choice for modern armed forces. In cyber warfare, the attacker tries to remain dominant, which has led militaries to focus more on developing offensive cyber capabilities. Moreover, cyber operations are conducted at a high speed with a global strike range, and a "target-rich environment" is available to the attacker,[36] making cyber warfare the ideal domain of warfighting in a digitized world.

Another dimension of cyber warfare's role as a force multiplier or enabling component is based on its asymmetric nature. For example, a smaller and conventionally weaker military cannot compete with a superpower with a high-end conventional military and a larger force. However, by retaliating in an asymmetric realm through the use of unconventional cyber warfare capabilities, it can potentially gain significant advantages over its adversary.[37] In addition, other concepts such as deterrence and economic interdependence also do not undermine the use of cyber warfare by militaries because of the anonymity of the attacker (via masking) and the lack of authentic attribution.[38] Cyber warfare also adds to the offensive capabilities of militaries because of its rapidly changing nature. Whenever effective countermeasures for a particular cyber weapon are created, militaries tend to develop new cyber weapons for offensives to both gain an advantage and undermine the enemy's security.[39]

American Doctrinal Induction of Cyber Warfare: Military Operations and Their Effects

At the beginning of the 21st century, the Office of the Joint Chiefs of Staff of the U.S. published a policy document named *Joint Vision 2020* for its armed forces to outline a road map for policy-making and operations from a tactical to strategic level. The *Joint Vision 2020* recognized the importance of asymmetric information technology capabilities that might prove detrimental to American national interest and simultaneously reveal vulnerabilities of the country. The technological imbalance would pose a full-spectrum threat to the U.S.: The role of communications channels, information technology, and computer networks would snowball to a large extent, which would ultimately lead to a cyberspace strategic competition. As a result, the U.S. military must equip itself to achieve full-spectrum dominance and conduct cyber warfare. [40]

By 2011, the U.S. had come up with an *International Strategy for Cyberspace* to identify the threats, develop cyberspace capabilities, mitigate the challenges, and achieve desired stability in the domain.[41] The document recognized disruptive and threatening attacks like blocking a website, international network disruption, and attacks on economic infrastructure, etc. as challenges to the national and economic security of the country for which its civil and armed forces must develop defensive and offensive cyber capabilities.[42] The *International Strategy for Cyberspace* also highlighted that the U.S. would develop capabilities to deter and dissuade its adversaries; the country would establish a robust cybersecurity and cyber warfare infrastructure to withstand attacks and afterward launch offensive operations in the cyberspace domain. Moreover, under its "inherent right to self-defense," the U.S. also outlined that it would provide cyberspace deterrence to its military treaty partners if required.[43]

The strategy also called for engaging in the military sphere to protect critical infrastructure against disruption, to prevent military operations from being dominated in operating environments, and to safeguard the economic and defense industrial base. Michael Daniel, a former White House cybersecurity coordinator, stressed to computer security practitioners that it was essential for role-players to defend the economic interests of the U.S. from cyber warfare.[44] The strategy also prioritizes the use of cyberspace for achieving global situational awareness, decreasing response time in areas of contingencies, and initiating cybersecurity exercises with partners.[45] In the global strategic landscape, the U.S. military aligns its cyber warfare strategy with its allies and has established defense-in-depth in the cyberspace domain against states and non-state actors.[46]

For the U.S., incorporation of cyber warfare did not remain confined to its doctrines; rather specific military units, which were later converted into USCYBERCOM, were tasked to conduct cyberattacks on specified targets. One

China correlates its cyber warfare/security strategies with ancient war concepts –it connects Sun Tzu's opinion about deceptive and passive war with cyber warfare

of the most famous cyber operations was conducted jointly by the U.S. military and Israeli forces against Iranian nuclear power plants. The cyber operation disabled Iranian nuclear plants' centrifuges to curtail weapon-grade uranium enrichment and was later termed 'Stuxnet' (2010).[47] It was in 2013 when the U.S. military, for the first time, declassified the *Joint Publication on Cyberspace Operations*. This officially publicized the employment of cyber warfare by American armed forces and the use of cyberspace for strategic competition.[48] The publication highlighted the use of cyberspace by the American military for offensive cyber operations (OCO), defensive cyber operations (DCO), counterintelligence (CI), DOD information network operations (DODINO), and cyberattacks.[49]

The *Joint Publication on Cyberspace Operations* also called for integrating the tri-services with technologically enabled command and control structures. Cyber operations are also designed to identify gaps between adversaries and the U.S. military during mission analysis. In addition, cyberspace operations were also directed to facilitate the integration and synchronization of weapon systems with the operational requirements and capabilities.[50] Since 2010, the U.S. published several documents on cyberspace operations, the establishment of multiple Cyber Mission Forces (CMF), the operational road map for USCYBERCOM, USCYBERCOM's commander's vision so on and so forth.[51]

In 2016, the Obama Administration tasked USCYBERCOM to conduct cyber warfare against the ISIS, about which then-Secretary of Defense Robert O. Work said, "We are dropping cyber bombs."[52] To carry out the covert offensive cyber operation named "Glowing Symphony,"[53] new cyber units were established under USCYBERCOM. The cyber operations were directed to amend the electronic communication of militants and redirect their missions. Former President Barack Obama, while talking about cyber warfare against ISIS said, "Our cyber operations are disrupting their command and control and communications."[54] The operational tactics involved coordinated phishing emails and the insertion of malware in ISIS servers, through which 10 core accounts of ISIS members launched propaganda campaigns. USCYBERCOM was able to penetrate the network and delete ISIS files, IPs, and accounts, denying the militants of any possible information retrieval.[55]

The command vision for USCYBERCOM published in 2018 was titled, *Achieve and Maintain Cyberspace Superiority* to highlight the importance of this domain for the U.S. military. The document not only crafted a road map

The Chinese military has not been associated with any cyberattack on conventional military targets. However, the country has been linked to cyber espionage for gathering sensitive information across civil, economic, and military sectors

for the cyber command but also outlined that the military options for the operational commander would also be expanded.[56] USCYBERCOM must curtail adversaries' cyber offensives at the point of origin and continue to operate for tactical, operational, and strategic advantages. This should involve the disruption of adversaries' action[57] so the U.S. can conduct cyber warfare unceasingly to achieve and maintain a three-layered cyberspace dominance cycle. The command vision also calls for the cyber command to augment the Joint Force by delivering operational and strategic advantages to it. A persistent engagement of the American forces in cyberspace weakens its adversaries by imposing tactical friction, hindering their desired strategic outcomes and adversely affecting their plans.[58]

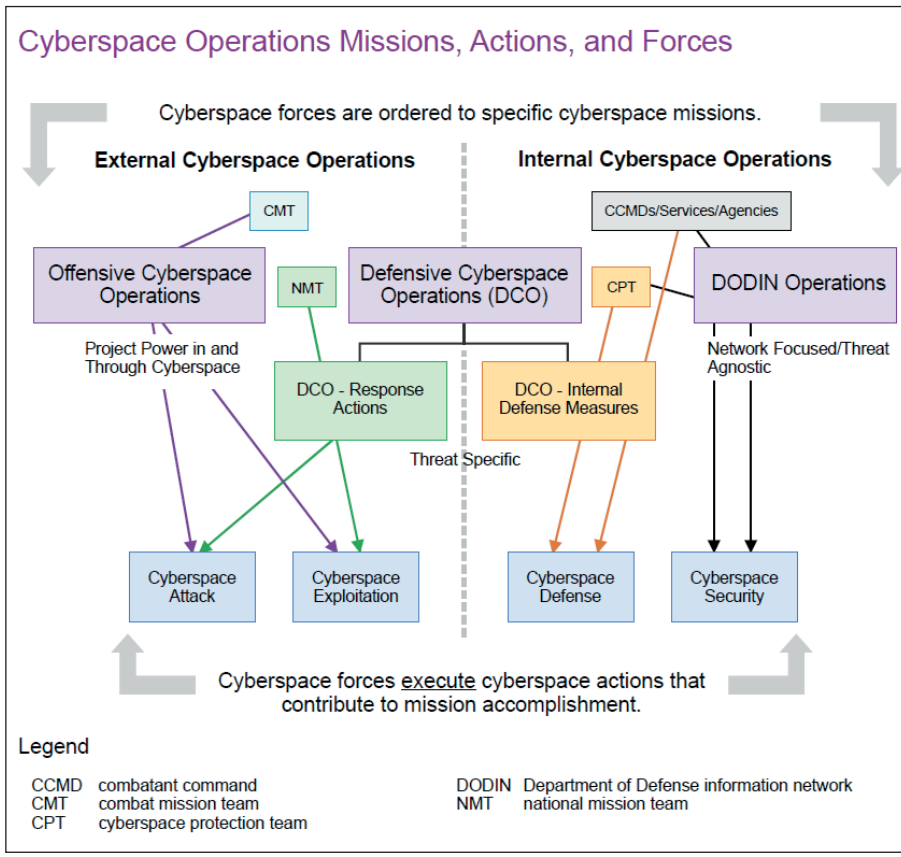
The command vision is further dictated by the following imperatives that support American military operations in cyberspace and enable its military to implement challenges in all competing domains:[59]

i. Develop and maintain cyber, emerging, and disruptive technologies earlier and more effectively than adversaries to gain advantages as desired,
ii. Prepare American forces for joint operations and integrate cyberspace capabilities across all military domains,
iii. Enhance the scope of cyberspace activities to support joint forces and simultaneously integrate intelligence, information, and communication operations,
iv. Manage cyber technologies for quick and agile full-spectrum operations and draw support for decision-making, policy-making, and operational concepts,
v. Expand the horizon of partnerships with allied militaries, academia, and experts in the cyberspace domain and use these partnerships for the identification and understanding of cyberspace advances to cope with any shortcomings.

The Office of the Joint Chiefs of Staff revised the *Joint Publication on Cyber Operations* in 2018. The revised version outlined several transformations in the policy and operational scope. First of all, it interrelated the tri-layered cyberspace structure in a way that all three (physical network, logical network, and cyber-persona) completed the operational cycle of cyberspace.[60] The 2018 version of the publication recognizes the strategic competition with nation-states

and also underlines that the nation-states might directly conduct cyber operations or outsources them to third parties.[61] It also tasked various units under USCYBERCOM with dedicated activities. The primary external cyber operations were directed to the combatant commands and associated mission teams, while the core activities for internal cyber operations were given to the Department of Defense Information Network (DODIN) and associated mission teams.[62] Figure 3 shows the complete cycle of missions and forces designated to carry out particular actions.

Figure 3: The Cyberspace Operations' Mission Cycle



Source: *Office of Joint Chiefs of Staff*[63]

To complement the military doctrines, the U.S. also published a national cyber strategy, under which it stated that the country would employ all kinds of resources, including military (be they kinetic or cyber), for prevention, mitigation, and deterrence of cyber operations against Washington. It also called for establishing a cyber deterrence initiative through which the U.S. would build a coalition force and devise tailored strategies against adversaries according to their strengths and prevailing environment.[64]

Chinese Incorporation of Cyber Warfare: Doctrinal and Operational Analysis

In its strategic competition with the U.S., the People's Republic of China (PRC) has invested heavily in its armed forces to achieve conventional parity. During the first decade of the 21st century, the conventional gap was so enormous that the Chinese military explored unconventional options to offset the U.S. military superiority. To address the conventional challenges, Chinese military strategists opted for the development of disruptive technologies and cyber warfare capabilities to counter conventional military threats.[65] As mentioned earlier, China termed cyber warfare as "information warfare," which, in 2004, it changed the basic aim of the preparations for military struggle (PMS) from "winning local wars under conditions of modern technology" to "winning local wars under conditions of informatization."[66] This particular understanding was added to and elaborated on by Beijing's National Defense Strategy (2004) when it was highlighted that "informatization" had become a cardinal to act as a force multiplier and enhanced the warfighting capabilities of the military.[67]

Another cardinal component in Chinese cyber warfare policy revolves around establishing processes and developing measures to neutralize any hostile information warfare plans based on network technologies. In doing so, Beijing focuses primarily on "counter-espionage" structures that would operate against foreign intelligence services. Moreover, the country acknowledges cyber warfare as a supporting domain for enhancing military capacity pertinent to building plans against cyberattacks and other threats in the cyberspace field. Similarly, China correlates its cyber warfare/security strategies with ancient war concepts –it connects Sun Tzu's opinion about deceptive and passive war with cyber warfare. This particular threat focuses are shaping the Chinese military outlook and its security policies in the contemporary world order.[68]

The Chinese military has not been associated with any cyberattack on conventional military targets. However, the country has been linked to cyber espionage for gathering sensitive information across civil, economic, and military sectors. The "Titan Rain" attacks conducted in 2007 on the United Kingdom's (UK) Foreign and Commonwealth Office and the U.S. Department of Defense were attributed to China. Similarly, the 2009 "GhostNet" attacks directed at large-scale spying on various targets, including government departments and strategic sites, were linked to China.[69] In line with the incidents mentioned above and various documents published by the PLA, it has been noted that cyber warfare is not considered merely a force multiplier on the battlefield but an unconventional warfare weapon. This unconventional weapon is considered to preclude conventional military action against adversaries and dominate them in cyberspace. Hence, cyber warfare can be termed as a "preemption weapon."[70]

The *Science of Military Strategy* published in 2013 became the first official document in which China publicly addressed cyber warfare through the military lens. It outlined that the PLA recognizes cyberspace as a "domain of military struggle."[71] This was again reiterated in the country's national defense paper titled *China's Military Strategy* published in 2015. The paper called for the country's military to build robust cybersecurity and cyber warfare infrastructure and an operationally ready force as Beijing was vulnerable to grave cyberspace threats. It also recognized the high-intensity international cyberspace strategic competition and the fact that many countries continue to build their "cyber military forces."[72] These developments pressured China to fuse cyberspace with other elements of national security and subsequently build cyber capabilities to not only defend itself but engage in offensive operations based on the continuously changing cyber warfare approaches. The Chinese view of cyber warfare converges with the American interpretation of cyber warfare on the point that both consider it to have a significant role not only in the military domain but for the broader national security components.[73]

Cyberattacks are not only aimed at conventional forces but are launched on unconventional targets, including satellites

Several publications highlight the adoption of cyber warfare and the development of cyber technologies by the PLA. The PLA's electronic warfare and SIGINT operational concepts have expanded in scope and have integrated cyber warfare. Cyberattacks are not only aimed at conventional forces but are launched on unconventional targets, including satellites. To support these activities, China plans to establish an information complex to ensure the integration of combat strikes, electronic warfare, cyber systems, and reconnaissance operations.[74] Moreover, cyberattacks have been added to the offensive operations category to achieve strategic objectives. Against its adversaries, the PLA aims at degrading, disrupting, and/or controlling the enemy's information systems[75] to dominate the observe-orient-decide–act (OODA) loop.[76] Major General Qiao Liang of the People's Liberation Army Air Force (PLAAF) Command College and Wang Xiangsui, a professor and retired senior colonel of the PLA, introduced the idea of cyber warfare being employed against critical network infrastructures, including command and control systems, as early as 1999 in the book *Unrestricted Warfare: China's Master Plan to Destroy America*.[77]

Later on, Xu Rongsheng, chief of cybersecurity research at the Chinese Academy of Sciences, upheld this approach by adding telecommunication power systems to the targets of cyber warfare in wartime.[78] Similarly, Lieutenant General Liu Jixian of the PLA's Academy of Military Sciences also called for the Chinese military to carry out cyber warfare and develop critical cyber technol-

With the employment of high-end military technologies, autonomous weapon systems, and sophisticated cyber warfare capabilities, the associated vulnerabilities also increase

ogies for combat purposes, including enabling precision-weapon attacks or paralyzing airports or naval ports.[79]

China has actively monitored its internet sphere, particularly social media platforms, to regulate the dissemination of information and data. These surveillance activities started in the wake of large-scale protests in Iran after the 2009 presidential election, the Arab Spring of 2011, and the London Riots in 2011.[80] In the policy circle, strategists and PLA authors emphasize the integration of all domains of warfare to conduct seamless operations. With the integration of communication networks, computers, sensors, and autonomous systems in tri-services, it is debated that the Chinese military would maintain a "dominant battlefield awareness" while having the leverage to exploit communication networks, command, and control hubs, electronic logistic lines, etc. of its adversaries.[81] Lu Linzhi, a retired major general from the PLA, considered the use of cyber warfare beneficial for China as the American forces heavily rely on information systems and communication networks for conducting their operations. If the PLA cyber warfare forces hack or disrupt the American systems and cause a short-term or permanent delay to their operations, the PLA can use it as leverage to strategically dominate the conflict and decision-making cycle for a decisive victory.[82]

In its 2019 *Defense White Paper*, the People's Republic of China identifies a new wave of strategic competition as a result of the U.S.'s readjustment of its security and defense policies. Heavy investment by the U.S. in the cyber domain along with others undermines global strategic stability for which it becomes imperative for China to develop top-notch cyber technologies and compete with its adversaries in the said domain.[83] The *White Paper* also highlights new considerations in the new era, stating that cyberspace is one of the core pillars of China's security interests that the country should strive to defend. Chinese armed forces continue to develop offensive and defensive cyberspace capabilities at a rapid pace along with reinforcement of national cyber defense infrastructure to protect sensitive information and maintain cyber sovereignty.[84]

In the operational realm, the PLAAF (Air Force), PLAN (Navy), Secondary Artillery Force (SAF), and all other branches of the Chinese military have been linked to the Third Department to conduct cyber operations and surveillance on foreign communications. Moreover, the Third Department also carries out functional orientation for monitoring communication networks from a tactical to a strategic level.[85] The former commander-in-chief of the U.S. Pacific Command blamed the People's Republic of China for cyberattacks and intrusions targeting

the Pacific Command's networks and computer systems aimed at stealing data.[86] Chinese technology and telecommunication companies have also been allegedly involved in cyber espionage: Huawei Technologies was blocked by the U.S. because of its links with the Chinese military. Many Chinese electronics manufacturers have reportedly installed viruses in devices to fetch information.[87]

Implications for International Security

The contemporary strategic landscape continues to remain volatile. The instability today is not only dependent on conventional components but also unconventional factors that intensify the strategic competition among different actors, especially military powers. The role of cyber warfare in the strategic, operational, and tactical realms has matured to an extent that its applications have become entrenched in military operations. The international security infrastructure in terms of doctrinal development, revamping of alliance structures, and operational application of militaries, force postures, and future planning has altogether been transformed by the weaponization of cyberspace, the cyber arms race, and the practical manifestation of cyber warfare by countries.

Competing on all military fronts, the cyberspace military rivalry between the U.S. and the PRC is intensifying with each passing day and is resulting not only in cyberspace strategic instability but akin to nuclear weapons, it is also fueling the cyberspace security dilemma. With the employment of high-end military technologies, autonomous weapon systems, and sophisticated cyber warfare capabilities, the associated vulnerabilities also increase. The most highlighting characteristics of cyber warfare in retrospect involve attribution, anonymity, and the fact that non-state actors also possess these technologies. It can safely be said that if any non-state actor conducts cyber operations against either country and its threshold crosses the limit of an all-out war or does unacceptable damage to the critical infrastructure, it can snowball into a nuclear war or even a third world war within a couple of minutes.

Another aspect of the increased cyberspace strategic competition involves regional security structures. The respective transformation of alliances and the transfer of cyber technologies by both the U.S. and the People's Republic of China have affected the military balance and deterrence stability in many regions of the world. For example, in the Asia-Pacific, the new alliance outlook involves members of the Quadrilateral Security Dialogue (Quad), including Japan, Australia, India, and the U.S. against China and Pakistan. These two military poles have repercussions for global stability in general and in particular for regions like South Asia, the South China Sea, and so forth. To analyze the effects, it is worth noting that in its Indo-Pacific Strategy Report (2018), the U.S. aimed to build cyberspace alliance networks to curtail its adversaries'

progress in the domain. Moreover, it aims to multiply the effects of its cyber operations by launching coordinated attacks with its allies against its stated adversaries, including China.

Furthermore, at the regional or sub-regional level, trickle-down effects are witnessed: having the U.S. armed forces and their logistics and technological support at its back, countries like India engage in intense competition against adversaries, including Pakistan and China. For Asia, the cyberspace competition may lead to an all-out nuclear war because of various factors: (i) any cyberattack might climb the escalation ladder because of ambiguous threshold levels; (ii) countries might conduct cyber operations to neutralize their adversary's navigation systems and afterward launch a conventional military offensive that might activate the nuclear flashpoint; (iii) cyber operations might cause unacceptable economic losses to a country that might be retaliated in form of a full-fledge war –specifically Pakistan, and (iv) above all, the geographical proximity of three nuclear-armed neighbors makes the region more volatile.

Cyber warfare also entails another aspect in terms of its conduct. Countries develop cyber capabilities to launch offensive operations against their adversaries while protecting their own structures and network systems against external attacks. To maintain sophisticated cyber warfare capabilities, countries use high-end computers, network-enabled systems, and other critical technologies. All of the above-mentioned technologies, despite being protected, are vulnerable to cyberattacks. The biggest threat at the state level is the launch of cyber warfare against a country's critical infrastructure that might have catastrophic effects on international security. The cyberattack on India's Kudankulam Nuclear Power Plant increased the chances of a large-scale war between India and Pakistan when at the beginning, Indian officials started blaming Pakistan for the operation. After, however, the attribution was given to some other entities, and the incident was de-escalated because no losses were reported.

Conclusion

Inherent differences in general approaches toward cyber espionage, the role of international law in cyberspace, and the militarization of cyberspace prove detrimental to international security as all the countries are dependent on either Washington or Beijing for cyberspace activities. Similarly, the development of dual-use technologies in telecommunications equipment and the integration of AI technology in warfare have also created confrontational scenarios for both countries time and again.[88] To understand the global cyber-threat matrix, it is important to note that countries gauge cyber threats differently depending on their capabilities and dependence on technology. Technologically advanced countries rely more on cyberspace because their transportation

networks, power-generation processes, telecommunications structures, banking and finance, government institutions, and military services depend extensively on data networking. The slightest disruption in the technology infrastructure can bring chaos to society and handicap the military from operating. In countries less reliant on cyberspace, associated vulnerabilities automatically become less viable and the domain is used for political gains rather than the disruption of facilities and institutions.[89]

Technologically advanced countries rely more on cyberspace because their transportation networks, power-generation processes, telecommunications structures, banking and finance, government institutions, and military services depend extensively on data networking

Cyberspace has redefined the threat matrix of international security: from being employed at battlefields to taking wars to the enemy's home front, scenarios of cyber conflict can include compromising software, algorithms, etc. to neutralizing hardware threats such as electromagnetic weapons. Cyberspace threats might not involve getting unauthorized access to conventional or unconventional missile arsenals of adversaries but could lead to conflicts having disruptive effects on countries, from strategic to operational levels and also threaten individuals of the countries.[90]

The significance of cyber warfare capabilities for militaries can also be gauged by former Chairman of the U.S. Joint Chiefs of Staff General Martin E. Dempsey's statement in which he said, "We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse." To connect this statement with the global security landscape, it is to note that 20 countries (or more) have established dedicated military units to conduct cyber warfare.[91] Cyber warfare is not only detrimental to an adversary's military but can also handicap its economy on which all the other elements of national power are dependent.[92] Hence, militaries can target a non-military target through operations in the cyberspace domain and achieve strategic results as the cyberspace domain is not as regulated as battlefields or warzones.

Maintenance of an embedded cyberspace infrastructure in the militaries, its interconnectedness with the economic junctions, and the development of cyber weapons became game changers for the international security architecture. Traditional structures, although interoperable and running parallel, are dominated by cyber weapons, disruptive technologies, and AI-driven equipment. For example, in a joint mission, a cyber warfare unit can not only deprive fighter jets of navigation systems, take control of their electronic weapons, and neutralize naval threats by compromising their computers but can also par-

alyze the army by hacking into the C5ISR and satellite systems and cutting off their eyes and ears. The possibility of a successful cyber campaign in the above-mentioned war scenario is 100 percent as all of this would take just a couple of seconds or a few minutes, at maximum, for a cyber warfare unit.

To conclude, the utility and application of cyber warfare make it the ultimate weapon of choice along with its offshoots such as AI, electronic warfare, and others. In the future, any country lagging in developing cyber capabilities could face detrimental results for its national security. Similarly, conflict and war zones would also be characterized and dominated by cyber warfare, which would require extensive work in capability development, preparedness, and R&D.

Endnotes

1. Margaret Kosal, "Disruptive and Game Changing Technologies in Modern Warfare: Development, Use, and Proliferation," in Anthony Masys (ed.), *Advanced Sciences and Technologies for Security Applications*, 1st ed., (Atlanta: Springer International Publishing, 2020).

2. "Command History," *U.S. Cyber Comment*, (May 8, 2019), retrieved from https://www.cybercom.mil/About/History/.

3. Sarmad Ali Khan, "Cyber Warfare as a Non-Kinetic Threat: Implications for Pakistan," *New World Architecture of Economy and Security*, (İstanbul: TASAM, 2020), pp. 482-483.

4. Khan, "Cyber Warfare as a Non-Kinetic Threat: Implications for Pakistan."

5. Katie Lange, "Cybercom: How DOD's Newest Unified 'Cocom' Works," *U.S. Department of Defense*, (October 12, 2018), retrieved from https://www.defense.gov/Explore/Features/Story/Article/1660928/cybercom-how-dods-newest-unified-cocom-works/.

6. Lange, "Cybercom: How DOD's Newest Unified 'Cocom' Works."

7. C. Todd Lopez, "Commander Discusses a Decade of DOD Cyber Power," *U.S. Department of Defense*, (May 21, 2020), retrieved from https://www.defense.gov/Explore/News/Article/Article/2193130/commander-discusses-a-decade-of-dod-cyber-power/.

8. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," *U.S. Department of Defence*, (2018), retrieved from https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, pp. 1-2.

9. Katie Lange, "Cybercom: How DOD's Newest Unified 'Cocom' Works," *U.S. Department of Defense*, (October 12, 2018), retrieved from https://www.defense.gov/Explore/Features/Story/Article/1660928/cybercom-how-dods-newest-unified-cocom-works/.

10. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," pp. 3-4.

11. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command."

12. "Indo-Pacific Strategy Report," *U.S. Department of Defence*, (June 1, 2019), retrieved from https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF, p. 8.

13. "Indo-Pacific Strategy Report," p. 13.

14. Piret Pernik, Jesse Wojtkowiak, and Alexander Verschoor-Kirss, "National Cyber Security Organisation: United States," *NATO Cooperative Cyber Defence Centre of Excellence*, (2016), retrieved from https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf.

15. Lopez, "Commander Discusses a Decade of DOD Cyber Power."

16. Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges*, Vol. 7, No. 2 (2011), pp. 81-103.

17. Ball, "China's Cyber Warfare Capabilities."

18. Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Emerging Threat," *Defense Technical Information Center*, (November 1, 2001), p. 6.

19. Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare," *Defense Technical Information Center*, (March 1, 2014), p. 3.

20. Wortzel, "The Chinese People's Liberation Army and Information Warfare," p. 4.

21. Larry M. Wortzel, "The Chinese People's Liberation Army and Information Warfare," *Fort Belvoir, VA: Defense Technical Information Center*, (March 1, 2014), retrieved from https://doi.org/10.21236/ADA596797.

22. Ball, "China's Cyber Warfare Capabilities," p. 81.

23. Yao Jianing, "White Paper 2014," *Ministry of National Defense of The People's Republic of China*, (2014), retrieved from http://eng.mod.gov.cn/publications/2016-07/13/content4768294.htm.

24. Li Jiayao, "China's National Defense in the New Era," *Ministry of National Defense of the People's Republic of China*, (July 24, 2019), retrieved from http://eng.mod.gov.cn/publications/2019-07/24/content_4846452.htm.

25. Ball, "China's Cyber Warfare Capabilities," p. 83.

26. Anthony H. Cordesman, Arleigh A. Burke, and Max Molot, "Advanced Modernization and Preparation for War: Informatized Warfare, New Force Elements, Cyber, Space, Logistics," *China and the U.S.: Center for Strategic and International Studies (CSIS)*, (2019), retrieved from https://www.jstor.org/stable/resrep22586.45.

27. Ball, "China's Cyber Warfare Capabilities," p. 84.

28. Eric Heginbotham, *et al*., "Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities," in *The U.S.-China Military Scorecard*, *Forces, Geography, and the Evolving Balance of Power 1996-2017*, (RAND Corporation, 2015), pp. 260-266.

29. Anatasia Latenkova, "Invisible Battleground: The Reality of Cyber Warfare," Bachelors Thesis, State University of New York, 2017, pp. 7-8.

30. "Chapter Ten: Military Cyber Capabilities," *The Military Balance 2020,* Vol. 120, No. 1 (2020), pp. 515-518.

31. Joseph S. Nye, "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" *Bulletin of the Atomic Scientists*, Vol. 69, No. 5 (September 1, 2013), retrieved from https://doi.org/10.1177/0096340213501338, pp. 8-14.

32. Joseph S. Nye, "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" *Bulletin of the Atomic Scientists*, Vol. 69, No. 5 (September 1, 2013), p. 8.

33. Nye, "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?"

34. Murat Balcı, Göksel Küçükkaya, and Mustafa Canan, "Defining Military Levels for Cyber Warfare by Using Components of Strategy: Ends, Ways, and Means," *Research Gate*, (September 2016), retrieved from https://www.researchgate.net/publication/307923231_Defining_Military_Levels_for_Cyber_Warfare_by_Using_Components_of_Strategy_Ends_Ways_and_Means, pp. 3-4.

35. Fred Schreier, "On Cyberwarfare," *DCAF Horizon 2015 Working Paper No. 7*, (2015), retrieved from https://dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.

36. Schreier, "On Cyberwarfare," pp. 12-13.

37. Hanyu Chwe, "The Rise of Cyber Warfare: The Digital Age and American Decline," *Swarthmore International Relations Journal*, Vol. 44, No. 1 (January 1, 2016), retrieved from https://works.swarthmore.edu/cgi/viewcontent.cgi?article=1010&context=swarthmoreirjournal.

38. Chwe, "The Rise of Cyber Warfare: The Digital Age and American Decline."

39. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, (eds.), *2012 4th International Conference on Cyber Conflict Proceedings*, (Estonia: NATO CCD COE Publications, 2012), retrieved from https://ccdcoe.org/library/publications/4th-international-conference-on-cyber-conflict-proceedings-2012/.

40. "Joint Vision 2020: America's Military - Preparing for Tomorrow," *Policy Document*, (Washington, DC: National Defence University, 2000), retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf.

41. "International Strategy for Cyberspace," *The White House*, (May 2011), retrieved from https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

42. "International Strategy for Cyberspace," pp. 3-4.

43. "International Strategy for Cyberspace," pp. 12-14.

44. Brian M. Mazanec, *The Evolution of Cyber War - International Norms for Emerging-Technology Weapons*, (University of Nebraska Press, 2015), retrieved from https://www.nebraskapress.unl.edu/potomac-books/9781612347639.

45. "International Strategy for Cyberspace," pp. 18-19.

46. "International Strategy for Cyberspace," p. 20.

47. Khan, "Cyber Warfare as a Non-Kinetic Threat: Implications for Pakistan," p. 482.

48. "Cyberspace Operations," *National Security Archives*, (February 3, 2013), retrieved from https://nsarchive2.gwu.edu/dc.html?doc=2692126-Document-18.

49. "Cyberspace Operations," pp. 23-26.

50. "Cyberspace Operations," pp. 44-48.

51. "USCYBERCOM Documents Timeline," *National Security Archive*, (May 7, 2020), retrieved from https://nsarchive.gwu.edu/news/cyber-vault/2020-05-11/uscybercom-documents-timeline.

52. David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times*, (April 24, 2016), retrieved from https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

53. Louk Faesen, Tim Sweijs, Alexander Klimburg, and Conor MacNamara, "From Blurred Lines to Red Lines: How Countermeasures and Norms Shape Hybrid Conflict," *The Hague Centre for Strategic Studies*, (September 30, 2020), pp. 8-10.

54. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat."

55. Faesen, *et al.*, "From Blurred Lines to Red Lines: How Countermeasures and Norms Shape Hybrid Conflict," p. 20.

56. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," p. 2.

57. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," p. 3.

58. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," pp. 5-6.

59. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," pp. 8-9.

60. "Cyberspace Operations Joint Publication 3-12," *National Security Archive,* (June 8, 2018), retrieved from https://nsarchive2.gwu.edu/dc.html?doc=6379794-National-Security-Archive-Joint-Chiefs-of-Staff, p. 23.

61. "Cyberspace Operations Joint Publication 3-12," p. 31.

62. "Cyberspace Operations Joint Publication 3-12," p. 37.

63. "DOD Cyberspace: Establishing a Shared Understanding and How to Protect It," *Air Land Sea Space Application (ALSSA) Center,* (June 13, 2023), retrieved from https://www.alsa.mil/News/Article/2891794/dod-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/.

64. "National Cyber Strategy of the United States of America," *The White House*, (September 25, 2018), retrieved from https://nsarchive.gwu.edu/news/cyber-vault/2018-09-26/cyber-brief-white-house-department-defense-cyber-strategies, pp. 21-22.

65. Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, "On Cyber Warfare," *Chatham House*, (2011), pp. 6-7.

66. Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions?" *Carnegie Endowment for International Peace,* (April 1, 2019), retrieved from https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

67. Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions?" *IPI Global Observatory*, (March 22, 2019), retrieved from https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/.

68. Ali Burak Darıcılı and Barış Özdal, "Analysis of the Cyber Security Strategies of People's Republic of China," *Güvenlik Stratejileri Dergisi*, Vol. 14, No. 28 (December 12, 2018), pp. 1-35.

69. Cornish, *et al.*, "On Cyber Warfare," p. 8.

70. James C. Mulvenon and Richard H. Yang, *The People's Liberation Army in the Information Age*, (California: RAND Corporation, 1999), p. 183,

71. Mulvenon and Yang, *The People's Liberation Army in the Information Age*.

72. "China's Military Strategy," *Ministry of National Defense of the People's Republic of China*, (2015), retrieved from http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

73. Jinghua, "What Are China's Cyber Capabilities and Intentions?"

74. Wortzel, "The Chinese People's Liberation Army and Information Warfare."

75. Wortzel, "The Chinese People's Liberation Army and Information Warfare," p. 11.

76. The OODA Loop is a four-step decision-making cycle focused on the availability, contextualization, and assessment of information based on which an appropriate strategy is made and implemented. The OODA constantly changes based on the availability of more data.

77. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, (Echo Point Books & Media, November 10, 2015).

78. Wortzel, "The Chinese People's Liberation Army and Information Warfare," p. 16.

79. Wortzel, "The Chinese People's Liberation Army and Information Warfare," p. 20.

80. Jinghua, "What Are China's Cyber Capabilities and Intentions?"

81. Mulvenon and Yang, *The People's Liberation Army in the Information Age*, p. 182.

82. Mulvenon and Yang, *The People's Liberation Army in the Information Age*, p. 185.

83. Anthony H. Cordesman, "China's New 2019 Defense White Paper," *Center for Strategic and International Strategies*, (July 24, 2019), retrieved from https://www.csis.org/analysis/chinas-new-2019-defense-white-paper.

84. "China's National Defense in the New Era," *The State Council Information Office of the People's Republic of China*, (July 2019), retrieved from http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

85. Wortzel, "The Chinese People's Liberation Army and Information Warfare," p. 22.

86. Ball, "China's Cyber Warfare Capabilities," p. 82.

87. Ball, "China's Cyber Warfare Capabilities," p. 83.

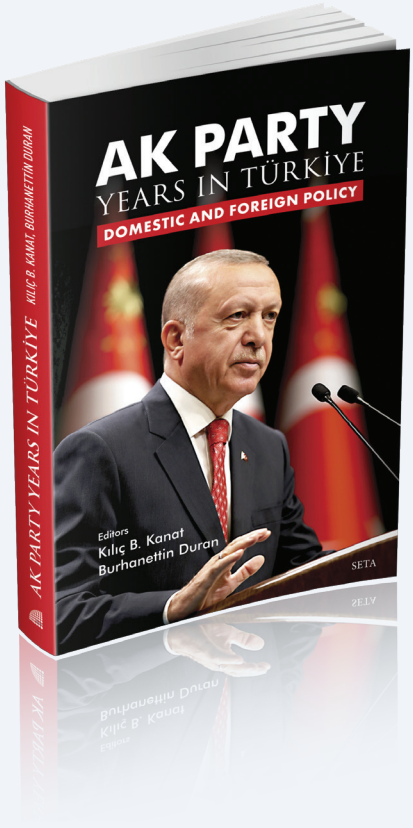
88. Ariel Levite and Lyu Jinghua, "Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?" *Carnegie Endowment for International Peace*, (January 24, 2019), retrieved from https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213.

89. Andrew N. Liaropoulos, "Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict," *Greek Politics Specialist Group*, No. 7 (April 2011), retrieved from https://www.academia.edu/612371/Cyber_Security_and_the_Law_of_War_The_Legal_and_Ethical_Aspects_of_Cyber_Conflict_Greek_Politics_Specialist_Group_Working_Paper_no_7_April_2011_.

90. Liaropoulos, "Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict."

91. Joseph S. Nye, "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" *Bulletin of the Atomic Scientists*, Vol. 69, No. 5 (September 1, 2013), pp. 8-14.

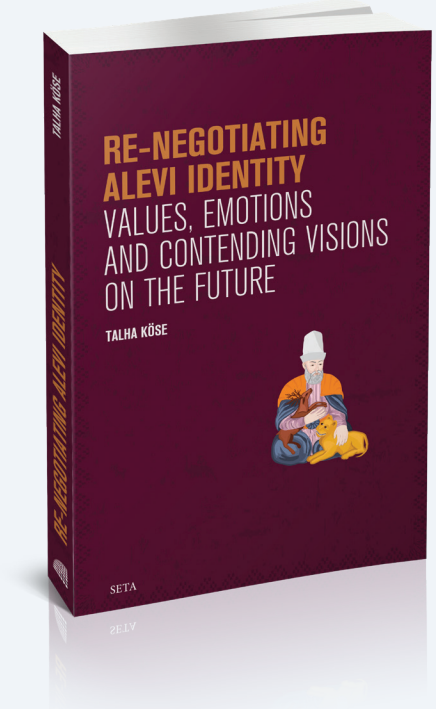
92. Nye, "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?"



AK Party Years in Türkiye | Domestic and Foreign Policy

May 2023 | Kılıç B. Kanat, Burhanettin Duran

The AK Party years in Türkiye have been truly transformational. When the party was established in 2001, the country was going through major economic and political crises. Today, under the leadership of President Erdoğan, Türkiye is a middle power with serious global ambitions. In the nearly two decades since its inception, the AK Party has been confronted with major domestic and foreign policy challenges.



Re-Negotiating Alevi Identity | Values, Emotions and Contending Visions on the Future

May 2023 | Talha Köse

This book investigates the transformation and the politicization of Alevi identity within the social and political context of post-1980 Türkiye. This study specifically focuses on the role of collective emotions and values in forming and transforming Alevi identity.