Dean Cheng

CYBER DRAGON

Inside China's Information Warfare and Cyber Operations

The Changing Face of War

PRAEGER SECURITY INTERNATIONAL

- Safeguarding China's expanding national interests, specifically within the realms of outer space, electromagnetic spectrum, and the maritime domain
- Helping ensure world peace[41]

Some of these "new historic missions" are of long standing. The PLA is a party army, the armed wing of the PLA. Therefore, sustaining the party's continued rule has always been a foremost task. Similarly, the PLA has long known that a fundamental responsibility was ensuring Chinese sovereignty and territorial integrity, that is, being prepared to retake Taiwan and enforcing Chinese rule over Xinjiang and Tibet in the face of separatist sentiments.

The task of safeguarding Chinese expanding interests, however, constituted a major revision of the PLA's responsibilities. As Hu noted, the PLA was now charged with preserving Chinese national interests beyond its traditional borders. In light of national development requirements and broader global trends, Hu observed that China's national interests and security were no longer limited to the traditional land, sea, and air. "Maritime security, space security, electromagnetic spectrum security," he noted, "are already vital regions for national security," where a number of major powers are seeking to secure advantage. In essence, Hu was expanding China's defined interests beyond its traditional borders, to the electromagnetic domain, the reaches of outer space, and the world's sea lanes.[42] In doing so, he was clearly elevating the information realm, of which the electromagnetic spectrum is an essential part and outer space is an integral part of its physical infrastructure.

For the PLA, Hu's instructions were a call to arms, to prepare for informationized warfare.

3 Chapter

Informationized Conflict: Maintaining Party Control amid the Information Revolution

For the PLA, preparing for informationized warfare complicated a modernization effort that had focused on mechanizing the world's largest army. Indeed, for much of the first decade of the 21st century, PLA writings observed that the PLA was still "half-mechanized, half informationized." For at least part of this period, the PLA appears to have simply sought to acquire more information technology, ranging from computers to better communications systems, while still converting its forces from light infantry to motorized and mechanized forces.

In relatively short order, however, the PLA recognized that informationization meant more than just adding a layer of information technology atop more mobile forces. Rather, it would require a thorough reexamination of the nature of conflict.

INFORMATIONIZATION OF CONFLICT

The PLA concluded that, just as informationization has affected global economy and society, it has also influenced the nature of war. War, from the PRC's perspective, is a function of not just military forces and politics, but also larger social, economic, and technological trends. According to PLA writings, the "shape of war" (*zhanzheng xingtai*; 战争形态) is a reflection of the dominant economic order of the day, which in turn affects the main types of weapons, military organizational structure, concepts of operations, and forms of combat.[1] These factors, in combination, help define the overall nature of warfare.

Historically, warfare has evolved as societies have progressed from agrarian to industrialized, and economies have shifted from agrarian, through feudal, to capitalist.[2] The weapons wielded have correspondingly transitioned from "cold weapons," that is, swords, spears, and other edged weapons, to "hot

weapons," that is, gun powder–based to mechanized forces. Concomitant with the changes in societal organization and technology have been shifts in military tactics and organizations. Thus, agrarian militaries relied on chariots and columns of foot soldiers. Feudal armies were comprised of knights and other mounted troops, as well as archers, pikemen, and other increasingly specialized forces, who could coordinate between mounted and marching forces. Industrial militaries included artillery and eventually tanks and aircraft, which in turn demanded more specialized training and more extensive logistics. For the same reason, the rise of the Information Age, marked by the widespread integration of information and information technology into all aspects of modern society and economics, also affects the nature of conflict, leading to "informationized warfare" (*xinxihua zhanzheng*; 信息化战争).

For the PLA, recognition of the growing centrality of information in modern warfare grew over the last years of the 20th and first years of the 21st century. Although the PLA was overhauling its approach to warfare throughout the 1990s, this involved incorporating more high technology and sophisticated equipment throughout the PLA and training its soldiers and officers to use that equipment. There was not, however, a focus on information and associated technology per se. Similarly, in authoritative PLA sources such as the 1997 edition of the *Chinese Military Encyclopedia,* and its 2002 supplement, there was no entry for the concept of "informationization" (*xinxi hua*; 信息化).

There was, however, already thinking in some quarters about the specific impact of advances in information technology on future warfare. The 1997 edition of the Chinese volume on military terminology includes an entry for "information warfare" (*xinxi zhan*; 信息战), describing it as

> the conflict activities conducted by the two sides in the information realm. It mainly involves securing information resources, seizing the initiative in the production, transmission, and management of information, disrupting the enemy's ability to transmit information, in order to create the conditions for constraining or fighting and winning conflicts.[3]

An analytical piece by a Chinese military professor in 2001 chastises Chinese military thinkers for failing to recognize that, besides the physical elements of soldiers and weapons, combat power would be increasingly generated through both greater access to information and information exploitation to link together forces.[4]

The military volume of a 2003 Chinese encyclopedia of phrases defined "informationized warfare" as arising when one or both sides in a conflict relies on informationized weapons and combat methods to undertake combat activities. Such warfare will typically include forces drawn from multiple services,

jointly conducted precision firepower attacks, computer network warfare, space warfare, special operations activities, and so on, in the various domains.[5] This suggests that the concepts associated with informationized warfare were already beginning to be discussed beyond purely military audiences.

Meanwhile, below the surface but shaping Chinese military modernization priorities was the need to concentrate on improving information technology and exploit its capabilities. This was reflected in the 2002 Chinese defense white paper, which stated that the shape of warfare was moving toward "informationization." In response, the PLA was charged with fulfilling the twin responsibilities of mechanization and informationization as it modernized.[6]

The subsequent 2004 Chinese defense white paper made even more references to the importance of informationized warfare. It noted, for example, that "the forms of war are undergoing changes from mechanization to informationization. Informationization has become *the key factor in enhancing the warfighting capability of the armed forces*."[7] PLA modernization, the white paper went on to note, would focus on improving "the operational capabilities of self-defense under the conditions of informationization."[8]

By 2005, the PLA had published a study guide for informationized warfare and associated operations, reflecting extensive internal discussion of information, information technology, and related issues. The PLA's 2011 volume on terminology describes "informationized warfare" as warfare where there are networked information systems and widespread use of informationized weapons and equipment, all employed together in joint operations in the land, sea, air, outer space, and electromagnetic domains, as well as the cognitive arena. In informationized warfare, the main form of conflict is between systems of systems.[9] As part of this systems-of-systems construct, informationized warfare is envisioned as informationized militaries, operating through networked combat systems, command-and-control systems and logistics and support systems.

In informationized warfare, information serves as both a force multiplier for people, matériel, and capability and a form of combat power itself. Older weapons that are modernized with modern sensors and communications equipment (e.g., the B-52 and the A-10 or adding laser guidance modules to "dumb bombs") can retain or even enhance their effectiveness. Improved command-and-control systems can better coordinate various forces. Better information can allow more effective allocation of limited resources, allowing one's own forces to be more flexible and agile. Information weapons, such as computer viruses, in turn, can paralyze an opponent's system of systems, causing them to disintegrate and decohere.

The focus of informationized warfare is establishing "information dominance" (*zhi xinxi quan*; 制信息权), the ability to establish control of information and information flow at a particular time and within a particular space.[10]

It entails the ability to collect more information, manage it faster, and employ it more precisely than the adversary.[11] By doing so, in the Chinese view, one can maximize the effects of all this newly available information. The side that enjoys information dominance can then seize and retain the initiative and force the adversary into a reactive mode, losing the ability to influence the outcome of an engagement. This exploits a key difference between mechanized warfare of the Industrial Age and informationized warfare of the Information Age. "Mechanized warfare focuses on physically and materially destroying an opponent, whereas informationized warfare focuses on inducing the collapse of the opponent's psychology and will."[12]

Establishing information dominance involves efforts that span the strategic to the tactical level. The knowledge required to establish information dominance includes an understanding of not only the adversary's information systems but also their key decision makers and decision-making processes. This entails significant intelligence gathering throughout peacetime. Because of the rapid, decisive nature of "local wars under informationized conditions," it is not possible to wait until the formal commencement of hostilities to begin preparations. At a minimum, identifying opposition capabilities and weaknesses must be undertaken in peacetime.

Nor can establishing information dominance be solely a military function. As the world has informationized, so has the global economy; consequently, key vulnerabilities may not be in military systems but in the financial system or critical infrastructures such as power or transportation. Because modern information networks are interconnected and given their extensive permeation, "information dominance" involves gaining access not only to enemy military networks but to essential nonmilitary ones as well. Civilian and commercial decision makers and the broader population are also vital targets. Similarly, it is essential to target not only an adversary's data but also the systems involved in data collection and management, and the users and analysts of that data as well.

For these reasons, successful defense against adversary efforts to establish information dominance makes enormous demands upon one's own information systems, both military and nonmilitary. Successful defensive efforts require countering adversary targeting of all three aspects of one's own information architecture, that is, data, systems, and users. Since information itself can be used as a weapon (beyond the incorporation of viruses and malware) by influencing its consumers, successful defense requires that information itself be monitored and information flow be tightly controlled.

Given the more expansive view of information's role, the human element is especially important. Chinese analysts note that the advent of more advanced weapons technologies did not necessarily lead to a change in war's basic nature. Instead, the core of informationized warfare is the expanded

range of abilities to influence and control an opponent's judgment and will to fight.[13] The ability to influence people, including their politics, thinking, morale and spirit, and psychology, can be as decisive and effective as the ability to interfere with databases or computer networks. Influencing an adversary through proper application of suitable information is embodied in the Chinese approach to political warfare.

POLITICAL WARFARE AS INFORMATIONIZED WARFARE

The Chinese conception of political warfare epitomizes its views of informationized warfare. "Political warfare" (*zhengzhi zhan*; 政治战) uses information to undertake sustained attacks against the enemy's thinking and psychology, to eventually subvert their will.[14] Successfully waging political warfare can help secure information dominance at its most basic level, influencing adversary thinking and perceptions. Conversely, information dominance is essential for successful political warfare; failure to establish information dominance opens the way to attacks on one's political stability.[15] From the Chinese leadership's perspective, there is a constant threat of "Westernization" and "splittism," endangering the nation's political security and the party's hold on power. This is at the root of Western calls for greater democratization and liberalization.

Although political warfare is mainly waged with strategic communications tools, including television, radio, the Internet, and news organizations, it is nonetheless considered *a form of warfare*. It envisions the use of information to attack opponents, eroding will, imposing psychological pressure, and influencing cognitive processes and the framework of perceptions. Because of the informationized condition of the global economy, political warfare efforts are no longer limited to frontline military forces but are applied against adversary populations and leadership. Political warfare is the weaponization of soft power.

Similarly, because modern information technology blurs the lines between peacetime and wartime, between military and civilian, and among strategy, operations, and tactics, political warfare is not limited to when hostilities have formally commenced and is not focused solely on military targets.[16] Instead, informationized warfare includes activities that are undertaken in peacetime, many of which are aimed at the adversary's political leadership and broad population. Informationized warfare, even more than Industrial-era mechanized warfare, encompasses the entire society of both sides.

PLA Concepts of Political Warfare Operations

Given the importance of political warfare, it should not be surprising that it is entrusted to the highest bureaucratic levels of the PLA. According to the

2003 "Political Work Regulations of the Chinese People's Liberation Army," and the subsequent 2010 revision, the General Political Department (GPD), one of the four General Departments that runs the PLA, is responsible for the conduct of political warfare. In particular, it is responsible for waging the so-called three warfares (*san zhan*; 三战)—public opinion warfare, psychological warfare, and legal warfare, the central methods of political warfare.[17]

The "three warfares" will be conducted in combination, as they are an integrated whole. Both individually and in concert, these political warfare efforts strive to shake the enemy's will, question their motives, induce divides and splits within the enemy's ranks, and constrain their activities. While ideally they might cause an opponent to concede the struggle entirely, more likely they will erode an adversary's will and thus reduce the ability to sustain any resistance to more kinetic operations.

Because of the difficulties in coordinating political warfare efforts with each other, as well as with both broader strategic measures (e.g., economic, diplomatic efforts) and military operations, the Chinese are emphatic about the need for coordination. This includes establishing a coherent plan for its conduct, incorporating not only the elements of political warfare (including the three warfares) but also other military, media, political, and diplomatic activities.

PLA efforts at political warfare are simplified and facilitated by vesting it within the GPD. Many GPD officers have undergone training in political warfare and indeed are specialists. Therefore, they will be planning and implementing operations for which they have been specifically trained. Moreover, the PLA contains an entire GPD chain of command that parallels the operational chain. This allows political warfare practitioners to oversee, coordinate, and integrate political warfare activities from tactical level to strategic, while maintaining methodological consistency and focus on specific goals.

The GPD's role will also facilitate coordination between political officers and staff and their operational counterparts of the General Staff Department (GSD). Because of the dual-control system (where authority is shared between GSD and GPD, especially through the political committee that runs the unit), there are extensive peacetime, day-to-day links between the two staffs as they manage the unit together.

While there is undoubtedly bureaucratic stove-piping between the two entities, there are also likely established means within individual units to coordinate activities, honed through peacetime interactions. This mutual familiarity is likely to pay off in wartime, in terms of integrating political warfare measures with other military operations.

The broad outlines of the political warfare effort, including "guiding principles" (*fangzhen yuanze*; 方针原则) and overall directives will come from the CCP Central Committee (in practice, the Politburo) and Central Military Commission (CMC). Higher-level commanders will take these principles, directives, and overall objectives and fashion plans of action for their level of command (joint campaign command headquarters [JCCH], group armies/military region air forces/fleets, etc.), while issuing guidance and directives for subordinate forces. Lower-level commanders, in turn, will draw up plans to fulfill their assigned operational missions and issue orders to their subordinates.

At each level of unit, specific political warfare efforts are developed by the unit's party committee, its political officer, and his staff. Organizationally, this means that the operational commander and main department heads, as well as the political officers of a unit, will participate in developing the political warfare effort, since all of them are part of the party committee. Again, at least theoretically this means that political warfare efforts are organically tied to more kinetic operations and activities. Military commanders are admonished, when laying out their operational plans, to integrate those plans with three warfare operations, making them all mutually supporting and complementary. This includes deconflicting resource demands and reconciling means and objectives.

The specific measures and plans for political warfare at the strategic and higher operational levels will likely be planned within the "political work office" (*zhengzhi jiguan*; 政治机关) contained in the joint JCCH. This office will usually be organized into a human affairs center, a propaganda and mobilization center, a military legal affairs center, a political warfare center, and the joint campaign party committee general office.[18] It will typically include the unit's top political officer and his staff, comprising three to five cadre, one of the unit's deputy operational commanders, and a senior member of the headquarters staff, as well as subordinate units' chief political officers.[19] The political work office is at the same level of importance as the JCCH's information operations center, firepower coordination center, joint logistics and safeguarding center, local support center, and so on. In some campaigns, depending on the forces committed, there may also be separate service political work offices, responsible for the individual services participating in a given campaign.

Not only will the main JCCH have a political work office, but there will also usually be a smaller counterpart office assigned to the forward command post of the JCCH. Headed by a deputy head of the political department, it will provide immediate, frontline political work support. These are more tactical-level activities, such as propaganda broadcasts and leaflet drops aimed at adversary frontline forces. Meanwhile, a reserve, rear-area command post will also have a political work office, headed by another deputy head of the unit's political department. This will often interact with the local civilian authorities, building upon the peacetime interactions that occur between a military unit's party committee and corresponding local civilian party committees. (For example, military districts, prior to the recent reform, were usually coterminous

with provincial boundaries.) The political warfare planners would be able to draw upon local, civilian personnel, equipment, and facilities (e.g., broadcasting stations, cyber specialists, Internet, and communications equipment).

Waging Political Warfare through the "Three Warfares"

Taken together, the three warfares seek to employ various types of information, for example, diplomatic, political, economic, as well as military, in a manner consistent with military strategic guidelines and objectives, to win the political initiative and achieve a psychological advantage. The aim is to strengthen one's own resolve while disheartening the adversary, since the lack of will makes even the most sophisticated weaponry irrelevant. An essential element of achieving this psychological advantage is to present oneself as the aggrieved party and holding the moral and legal high ground. Not only does this serve to stiffen one's own will, but it can be an important part of influencing bystanders and third parties.[20] Political warfare complements, but does not necessarily displace, traditional use of force.

Each of the three "warfares" employs information in a different manner to achieve these goals, but reinforces the other two. Psychological warfare exploits information by drawing upon political, economic, and cultural, as well as military elements of power. Information of each type can serve as a powerful weapon, influencing values, concepts, emotions, and context.[21] Legal warfare can build psychological support and sympathy among bystanders and erode an opponent's will by constraining the opponent's preferred courses of action for fear of legal repercussions. Public opinion warfare can directly build support, persuading domestic and foreign audiences of the justice of one's own cause and the success of one's own efforts, while undermining an adversary's attempts to do the same. In particular, the growth and expanded reach of media of various sorts makes public opinion warfare especially important, as it can have global effects. Broad domestic and international support, in turn, will generate psychological benefits for oneself and adversely affect the enemy.

Psychological Warfare

The central element of the three warfares is psychological warfare (*xinli zhan*; 心理战). This involves the application of psychological principles and methods to attack an opponent's psychology and erode the enemy's will to resist, while also engaging in psychological defensive measures to protect one's own will and encourage greater effort.[22] Psychological warfare pressures an opponent by employing information to affect its thinking, to create damaging or deleterious habits and ways of thinking, to reduce its will to resist, and perhaps even to induce defeatism and surrender.[23] At the same time, it seeks to limit the effect of enemy psychological warfare operations on one's own

troops, population, and leadership; building morale; encouraging greater resistance and effort; and strengthening will.

Psychological warfare employs a variety of measures including terror, intimidation, deception, enticement, as well as propaganda. The latter includes media warfare. Although psychological warfare draws on a variety of nonmilitary resources, it has always been a PLA responsibility, vested in the GPD's military political work structure.[24]

In many ways, all of the three warfares are ultimately aimed at influencing the adversary's psychology, whether by undermining popular support or imposing legal challenges and constraints. Psychological operations will be integral in future conflicts, affecting and influencing the very perceptions that inform decision making, from context to biases. Successful psychological operations in informationized warfare will generate repercussions at strategic, operational, and tactical levels of operations, influencing both military and civilian leaders and the masses, affecting the course and outcome of the conflict.

In the past, psychological warfare was more domestically or tactically focused and was primarily supplementing more kinetic operations.[25] It was very difficult to access an opponent's population; consequently, one sought to maintain domestic support or undermine enemy military forces through leaflets, battlefield loudspeakers, and so on. In World War II, radio broadcasts sought to undermine troop morale (e.g., "Axis Sally" and "Tokyo Rose"), but to limited effect. With advances in information technology, however, strategic psychological warfare is much more significant because of its broader reach.

By combining greater penetration and more comprehensive forms of psychological attack, modern psychological warfare practitioners have an unprecedented capacity for undermining an adversary's will and psychological balance. Psychological warfare can powerfully supplement traditional military means and effects. The rise of international news media, for example, provides a global messaging forum that magnifies strategic psychological warfare efforts. Similarly, international entertainment conglomerates influence audiences around the world, with attendant psychological impacts (e.g., subtly shaping perceptions and preferences).

Psychological warfare is not solely passive, however. Economic sanctions and blockades have long been employed to psychologically isolate an adversary as well as weaken its economy. Similarly, diplomatic measures such as withholding recognition of a regime underscore its isolation and vulnerability. The growth of global financial interconnectivity allows financial attacks, such as against an adversary's currency, generating psychological as well as economic repercussions. The Chinese believe modern technologies and techniques strengthen such measures, inducing "psychological shock and awe" (*xinli zhenshe*; 心理震慑).[26]

An additional method afforded by modern technology is the "information sanction" or "information blockade." By limiting the kinds of information an adversary can access, while preventing it from getting its own message out, a sense of strategic isolation is induced. This can erode domestic support and sap the will to resist. Chinese authors credit the United States with employing such methods against the Serbians in the Balkan conflict. NATO press conferences dominated global impressions of the situation, overwhelming Belgrade's ability to present its side. Meanwhile, NATO psychological warfare units broadcast messages into Serbia, employing a variety of platforms to transmit alternative television and other programming; they also exploited popular music and other means to obtain audience interest and generate public appeal.[27]

Similarly, Chinese analysts note how the United States imposed an information blockade on the Taliban, prior to intervening. This denied the Taliban information about American military preparations, while ensuring that the global understanding of the Afghan situation was seen through an American lens.[28]

By imposing an information blockade, the target's perceptions and viewpoints are more easily manipulated, since only limited information is available to it, and that may well be influenced or tainted. At the same time, the target is isolated, which may undermine its resistance, especially in the face of overwhelming force. The target's inability to spread its own message further heightens the sense of isolation, while limiting prospects for external support, which would afford both psychological and material relief. The spread of the Internet provides an important new venue for information blockades, raising the importance of imposing one but also providing an essential new means of doing so.[29]

Chinese examples of information blockades all commence *before* the formal onset of hostilities. This is typical, in the Chinese view, of most psychological operations. According to Chinese analyses, psychological warfare operations blur the line between wartime and peacetime, as well as between frontline and rear areas, military and civilian. Indeed, to be effective, such operations *cannot* be limited to wartime or just military targets. Instead, peacetime psychological operations are necessary to better understand an opponent and to lay the groundwork for more focused wartime efforts.

Peacetime applications of psychological warfare techniques influence and alter an opponent's unconscious, implicit views, making it more susceptible to coercion. An important approach is to employ various forms of strategic communications, including diplomatic efforts and economic influence, to foster a positive national image of oneself and increase foreign sympathy and support for one's own policies and goals. In addition, one should employ all types of communications, including various forms of media, to emphasize

one's own strengths, and the willingness to use it, to improve the ability to deter and coerce opponents.[30]

PLA writings also call for peacetime undermining adversary positions. This includes portraying others as fostering ill intentions and forcing them to react to various charges so their energy is dispersed and not concentrated on supporting their own goals. All the while, one must also be countering likely opposition efforts to foster their own image of strength and unity and defend oneself from their efforts at sowing demoralizing concepts.[31]

Wartime applications of psychological warfare shift the emphasis more specifically toward military targets and goals. The primary objective of wartime efforts is generating confusion, doubt, anxiety, fear, terror, regret, and exhaustion in an opponent, especially among senior military and civilian leaders. Ideally, this will induce neglect and maximize the chances of mistaken decisions or actions that can then be exploited. Wartime psychological warfare operations also aim to generate uncertainty and indecisiveness at all levels, degrading adversary decision-making processes. Interfering with an opponent's information systems, coupled with efforts to influence its decision makers, can create a strong psychological impact.

Another facet of wartime psychological operations is to sow discord and hopelessness in the enemy. Not only will this generate war weariness among enemy forces and populations, discouraging resistance, but can facilitate peace negotiations and induce more concessions. "When one defeats the enemy, it is not solely by killing the enemy, or winning a piece of ground, but is mainly in terms of cowing the enemy's internal heart."[32] This involves emphasizing information favorable to oneself and transmitting parallel messages via various forms of media, as well as through third parties, friendly elements in one's society, and so on.

Offensive psychological warfare operations must be complemented by defensive measures, since an opponent will be trying to undermine one's own forces, population, and leaders. It is essential to solidify popular support for the conflict, to highlight one's successes and the enemy's failures, and to instill confidence and support for the party and the state. This requires tight control over information flows in one's own society and insulating one's decision makers and decision-making processes from enemy information warfare efforts.

Both peacetime and wartime psychological warfare efforts require dedicated psychological warfare units and their staffing with suitably trained personnel. The units and personnel, moreover, must be familiar with modern information systems, as well as psychology, culture, and language, to maximize their effectiveness. Their training should incorporate "creation and application of information for psychological attacks; thoroughly understanding the enemy's military, social, and psychological weaknesses within likely conflict

areas, to facilitate focused creation of information for various types of [psychological] attacks; psychological warfare techniques and weapons, including broadcasting, battlefield loudspeakers, aircraft transmissions."[33]

Legal Warfare

Chinese analyses of legal warfare emphasize it is a central means of political warfare, supporting both psychological and public opinion warfare by "controlling the enemy through the law, or using the law to constrain the enemy (*yifa zhidi huo yong fa zhi di*; 以法制敌 或 用法制敌)."[34] Indeed, based on recent conflicts, the Chinese have concluded that "military warfare and legal warfare have already thoroughly combined," with legal warfare permeating conventional military operations, while military conflict intrinsically contains legal warfare.[35]

As with other forms of political warfare, legal warfare begins before formal commencement of military hostilities. By applying various types of legal information, including international and domestic laws, the laws of armed conflict, legal pronouncements, legal education, and law enforcement, Chinese leaders try to influence both foreign and domestic audiences. The objective is to garner support, deter action, and even influence military behavior, such as the choice of targets or weapons.[36]

Legal warfare involves depicting "one's own side is obeying the law, criticizing the other side for violating the law (*weifa*; 违法), and making arguments for one's own side in cases where there are also violations of the law."[37] The ultimate aim is securing the initiative in time of conflict by gaining the legal high ground, portraying oneself as more firmly grounded in legal standing, and implicitly being more virtuous and just. As one Chinese analyst observed,

> implementing "legal warfare" is to gain the right in warfare. Regardless of whether a war is just or not (*zhengyi yu fo*; 正义与否), the two sides in a war will both make every effort to develop "legal warfare," and seek out means of constructing legal bases for undertaking the war, and confirm that they themselves are the reasonable and legal side.[38]

The employment of legal information can play an important role prior to, during, and after the outbreak of formal hostilities. Legal warfare is integral to political preparation of the battlefield, employing legal information and arguments to influence various audiences in support of deterrent or coercive goals. It is especially important to broadly propagate Chinese legal positions and perspectives, so that they are "recognized by the international community."[39]

In peacetime, legal warfare influences domestic and foreign populations and leaders, weakening opposing coalitions while building support for one's own side. In wartime, it manipulates the rule of law in order to "destroy the will to fight by undermining the public support that is indispensable" for successful warfighting.[40]

Thus, Chinese passage of the 2005 Anti-Secession Law provides the political justification for any future move against Taiwan (or Tibet or Xinjiang) but also politically signals Chinese resolve to the native populations of these areas and any states or actors that might support them. Similarly, China's idiosyncratic interpretations of the UN Convention on the Law of the Sea signal not only China's position but its commitment to that position, which will potentially influence other claimants and players.

Indeed, the Chinese use of law enforcement vessels in many of its maritime territorial disputes is a form of both legal warfare and psychological warfare. It reduces escalatory pressures, since it employs civilian, not military, vessels. At the same time, the use of law enforcement vessels and agencies implicitly signals that a given piece of territory or water is Chinese—hence, it is subject to Chinese law enforcement as a matter of internal or domestic security rather than the military.

Beyond strategic uses of legal warfare, there are also operational and tactical benefits from the militarization of legal information and approaches. One potential use of legal warfare could be to delay American responses to Chinese actions. This could span a variety of options, such as filing motions relating to the War Powers Act or challenging the right to mobilize various American resources. In addition, there may be legal action in environmental, labor, and other arenas, beyond those directly linked to foreign policy and national security.

Chinese legal warfare efforts can also try to limit American access to foreign bases and facilities, essential for U.S. operations in the western Pacific. Such efforts would target any American ally and friends that might provide forward basing facilities, including Singapore, the ROK, the Philippines, and Thailand. These measures would likely be coordinated with pressurizing military activities (military overflights, nearby naval exercises), as well as economic actions, such as promises of expanded investment or threats of factory closures, and also diplomatic legal steps, such as support in other territorial or economic disputes (e.g., World Trade Organization cases). If successful against either the American or allied audience, such legal warfare measures could affect American deployments, reducing their ability to operate successfully against Chinese forces.

In wartime, American analysts have expressed concern that legal warfare efforts may induce excessive restraint in military operations. Military commanders may choose to err on the side of caution for fear of violating international law, especially the laws of armed conflict, and becoming liable to charges

of war crimes. Indeed, the American 2008 National Defense Strategy expresses concern about "growing legal and regulatory restrictions that impede, and threaten to undermine, our military readiness."[41]

Chinese analysts have reached similar conclusions. Legal warfare, in their view, can directly affect popular support for a conflict, both at home and abroad. One goal of legal warfare is

> to psychologically dissipate the other sides' fighting will in both the military and the civilian realms, while exciting one's own military and civilian passions and obtaining international sympathy and support.[42]

These analysts note, for example, the outcry after the bombing of the Al-Firdos bunker in the 1991 Gulf War and that "the substantial loss of human life and the serious violation of the laws of war" led to adverse political and moral consequences, which directly affected military planning and operations.[43]

Chinese analysts also see legal warfare as playing a significant role in the aftermath of conflict. Coupled with diplomatic and military measures, it can help consolidate wartime gains.

To achieve these ends, Chinese writings on legal warfare emphasize that it is a form of *warfare*. Therefore, it must be undertaken under a unified command organization, with a unified plan, coordinating among various political warfare measures, but also with more traditional, kinetic military measures.[44] These measures must also be undertaken in coordination with other strategic and operational goals.

Those coordinated legal warfare operations are *offensive* in character. They force an adversary to react and to devote time and resources responding. Chinese writings suggest that legal warfare measures would include

- Legal coercion/deterrence efforts, warning an opponent that it is under close scrutiny for possible violations of the laws of armed conflict, in order to impose self-constraint;
- Legal strikes, charging the enemy with operational activities in violation of international and domestic laws; and
- Legal counterattacks, highlighting enemy efforts at slanting or misrepresenting international law in its favor, unfavorably contrasting its conduct with one's own (in legal terms), and countering any enemy legal activities.[45]

By contrast, typical Western concepts of legal warfare are more *defensive*, driven by fears of legal sanction (and attendant loss of public support), that have often constrained exploitation of Western advantages.[46] Perhaps most controversially, early in the Afghanistan War, because the legal officer (JAG) on the American staff had concerns about civilians in Mullah Omar's convoy, an orbiting *Predator* drone was denied permission to attack. Omar therefore escaped.[47] More notably, in the context of informationized warfare, the U.S. Department of Defense reportedly did not employ certain cyber options against Slobodan Milosevic during the Kosovo conflict, because the legality of such actions was unclear.[48]

Public Opinion Warfare

Chinese analysts envision public opinion warfare (*yulun zhan*; 舆论战), also translated as "media warfare" or "consensus warfare," shaping targeted audiences through information derived and propagated by mass information channels, including the Internet, television, radio, newspapers, movies, and other forms of media. While news media play an important role in the Chinese conception of public opinion warfare, it is only a subset of the larger set of means available for influencing public opinion.[49] All these channels will transmit a consistent message to the intended audience, in accordance with an overall plan, to instill certain views and conclusions that are beneficial to oneself and detrimental to the adversary.

Public opinion warfare is an essential support for psychological warfare efforts, as it prepares audiences for the psychological warfare messages. Chinese analysts see public opinion warfare as an especially powerful element of informationized warfare. Because of the wide permeation of information technology, public opinion warfare can now reach every part of society.

The goal of public opinion warfare is to shape public and decision-maker perceptions and opinion, shifting perceptions of the overall balance of strength between oneself and one's opponent.[50] Successful public opinion warfare will influence three audiences: the domestic population, the adversary's population and decision makers (both military and civilian), and neutral and third-party states and organizations. It will preserve friendly morale, generate domestic and foreign support, weaken the enemy's will to fight, and alter the enemy's situational assessment. Public opinion warfare is both a national and local responsibility. Not only will the PLA engage in it, but so will the People's Armed Police, national and local media, spokespeople, netizens, and other groups.[51]

Public opinion warfare is an autonomous activity; it occurs independent of an actual, formal conflict. Put differently, it is always under way. According to Chinese analyses, the side that plants its message first enjoys a significant advantage influencing public opinion. Indeed, Chinese analyses repeatedly emphasize that "the first to sound grabs people, the first to enter establishes dominance (*xian sheng duoren, xianru weizhu*; 先声夺人，先入为主)." Essentially, the Chinese seek to define the terms of the debate and parameters of coverage. By presenting one's message first, the PLA expects to shape everyone

else's views. This will allow Beijing to underscore the justice and necessity of its operations, better display national strength, exhibit the superiority of its forces, and shake an opponent's will to resist.[52] By contrast, adversaries must overcome ideas that are already planted and taking root by Chinese public opinion warfare efforts. In a very real way, Chinese decision makers see public opinion warfare as being waged even in peacetime, as part of larger efforts shaping people's perceptions of the PRC. There is a constant effort to influence audiences to accept China's narrative and perceptual framework.

To maximize the effectiveness of public opinion warfare, all channels of information dissemination must be exploited, so that a given message is reiterated, reinforced by different sources and different versions. Public opinion warfare efforts embody the ideal of "combining peacetime and wartime operations; civil-military integration of resources; military and local resources unified (*pingzhan jiehe, junmin jiehe, jundi yiti*; 平战结合, 军民结合, 军地一体)."

The Chinese have established a Ministry of National Defense Information Office (MNDIO), responsible for engaging the press. This office is the main mechanism for disseminating China's position on military and security-related issues. It promotes the image of the PLA as a competent and capable force and tries to counter negative impressions, including that the PLA is a secretive organization. Established in 2008, spokespeople from the MNDIO have held monthly press conferences since 2011.[53]

Civilian resources play a prominent role in public opinion warfare, because there are substantially more civilian and commercial media assets, including broadcasting facilities, Internet users, and news organizations and reporters. Nonmilitary assets also often have better techniques and information than their military counterparts.[54] Where possible, public opinion warfare efforts will exploit the reputation and long-term presence (e.g., branding, established relationships) of those nonmilitary assets.

To be successful, public opinion warfare messaging must be flexible, incorporating shifts in strategic, political, and military contexts. Rather than a one-size-fits-all approach, different messages are tailored for different audiences. When engaging in public opinion warfare against what the PRC regards as secessionist elements, for example, "one must make distinctions between the more stubborn elements and the general populace."[55]

Careful preparation of the public opinion battleground in peacetime is essential. This requires understanding potential opponents' psychology and national moods, extensive research into tactics and methods, and developing public opinion warfare specialists. This is not limited to the news media; in the Iran–Iraq War, for example, Chinese analysts note that Iran linked news-based propaganda with religious outlets. Employing religious fervor helped bolster public morale in support of the state.[56] Such efforts, however, require a thorough understanding of target audiences. PLA writings consistently invoke the saying, "Before the troops and horses move, public opinion is already in motion (*bingma weidong, yulun xianxing*; 兵马未动，舆论先行)," emphasizing that public opinion warfare preparations must begin far in advance of formal hostilities.[57]

Indeed, it is not clear that public opinion warfare differentiates between peacetime and wartime. In the first Gulf War, the United States is said to have fully used its advantage in information dissemination to constantly bombard the Iraqi military and civilian population with various messages undermining Iraqi will (and especially to induce uncertainty in Saddam Hussein). This began long before the first cruise missiles struck or first air raids began. Chinese analysts note that before invading Afghanistan, Washington employed public opinion warfare mechanisms to create an antiterrorism coalition; gain international support; and allay concerns among Arab and Muslim nations.[58]

Defensive public opinion warfare efforts limit the impact of enemy public opinion warfare. These efforts entail strong education and news management efforts to minimize domestic popular exposure to enemy messages and to nullify the impact of those messages. Defensive public opinion warfare builds public skepticism toward external and internal criticisms of the government. Those criticisms that do leak through are countered by prompt, credible responses.

CHINA'S STRATEGIC INFORMATION DEFENSE

For the Chinese leadership, establishing information dominance requires preventing an adversary from exercising undue influence on the population. In the Information Age, this means that Chinese authorities must control the flow of information to the Chinese people, including via traditional media, but especially across the Internet and through social media channels.

Not only must the CCP counter foreign intrusions and interference, but it must also prevent *domestic* opponents from creating and spreading unrest. Social media platforms especially increase the potential of organized protests against CCP rule. The specter of internal and external opposition combining, or worse cooperating, makes information control a paramount priority and unfettered information flow a *strategic* threat.

The confluence of information technology expansion and the collapse of the Soviet Union affect CCP threat perceptions. After all, China's first connection to the Internet in 1994 occurred in the shadow of the USSR's collapse, which itself came on the heels of the Tiananmen Square massacre. The growing ability to share information, and act upon it, clearly poses burgeoning challenges to a Chinese leadership that has witnessed the collapse of global Communist ideology and significant domestic unrest. Chinese efforts to control the Internet and social media, with their extensive permeation and reach, should be seen as the equivalent of strategic homeland defense. The CCP's

determination to limit the vulnerability of the population (and therefore itself) to information weapons parallels civil defense measures to protect the population from nuclear weapons.

Especially important is control of social media platforms, which not only allow prompt dissemination of information to large audiences (akin to traditional media) but also can rapidly organize public opinion and even action. Indeed, preserving social control and preventing the population from engaging in unapproved action appears to be as important as censoring information outright. Rebecca MacKinnon observed in 2009 that Chinese governmental regulatory bodies base rewards and punishments "on the extent to which Internet companies successfully prevent groundswells of public conversation around politically inflammatory topics that might inspire a critical mass of people to challenge Communist Party authority."[59]

A subsequent study reached a similar conclusion, observing that "the purpose of the censorship program is to reduce the probability of collective action by clipping social ties whenever any collective movements are in evidence or expected."[60] Researchers found that Sina Weibo postings and other expressions were far more likely to be taken down and would be taken down faster, when they promoted collective action, for example, protests or gatherings. This was true *even if the messages supported the government's position*. "Whether or not the posts are in favor of the government, its leaders, and its policies has no measurable effect on the probability of censorship."[61]

The Chinese government closely monitors not only information but how that information is interpreted and acted upon. While it is not possible to totally control what is expressed, Beijing clearly tries to suppress unauthorized, popular reactions to that expression.

The central authorities' efforts are facilitated by the near total dominance of domestic providers, as well as governmental control of China's telecommunications infrastructure. By creating an indigenous set of social media platforms, rather than relying on foreign programs, Beijing can control not only what is transmitted via social media but also how that information travels over China's information and telecommunications networks. For example, Beijing has been able to shut down text messaging systems while maintaining cellular phone network operations. This has been essential, given the heavy reliance on mobile phones rather than landlines for general internal connectivity. Both private citizens and the government can continue to communicate, even when the government simultaneously clamps down on the ability to organize opposition, but the ability to create crowds is minimized.

In sensitive areas such as Tibet and Xinjiang, Chinese authorities have amply demonstrated both will and capability to prevent unauthorized and uncontrolled dissemination of information. In Tibet, both Internet and telephone connectivity has reportedly been spotty and uncertain since 2008 protests.

When protests about racial violence against Uighur workers in Guangdong became violent in 2009, Internet access was suspended across the entire Xinjiang Autonomous Region within hours. Limits on phone calls and text messaging followed.[62] Since then, there have been repeated shutdowns and disruptions of Xinjiang Internet and telephone service. However, in both areas, government agencies (e.g., police) and critical infrastructure such as finance and transportation have retained connectivity, reflecting the Chinese ability to wield a scalpel as well as a cleaver when controlling information.[63]

Through central control of physical infrastructure and promotion of indigenous software and platforms, China has created a fairly insulated, relatively controlled internal information environment, even as it is connected to the global information network. This is backed by an overlapping array of technical and human censors. These ensure not only that disseminated information is politically acceptable but any reactions can be channeled into acceptable forms.

The average Chinese citizen's view of the world, and even of China, is bounded by a pervasive, but not necessarily obvious, set of blinders. So long as they stay within those limits, they are free to enjoy the benefits of both an extensive internal information network and access to broader global resources. But should Beijing deem it necessary, the authorities can close some or even all of those shutters, in ways that few other authoritarian states can, because all of the levers are in Chinese hands.

Countering Political Warfare: Controlling Information

Especially important for the conduct of political warfare is mobilizing public opinion. This serves two functions. First, it builds and sustains support for the war effort and the top leadership. This, in turn, may signal an adversary of Chinese will and commitment, which may deter it from intervening or resisting Chinese actions. At the same time, mobilizing public opinion can help inoculate the population against the effect of local or strategic reverses. It is a means of manipulating the public's perceptions to avoid defeatism and uphold morale. This is especially important, given the likelihood of attacks on key Chinese economic, communications, and energy facilities.

Public opinion mobilization is a part of the larger information mobilization effort. It requires focused, targeted employment of information to obtain the intended effects.[64] This entails not only directly influencing Chinese public opinion but also shielding it from adversary efforts to influence and shape it.

Therefore, even as the Chinese authorities are waging political warfare against likely adversaries, they are also defending the Chinese population from such efforts. One essential concern is the ability of outsiders to exacerbate internal unrest and jeopardize CCP control. This is not a theoretical

concern, but instead reflects genuine worry among the senior Chinese leadership. The 2014 Chinese defense white paper, for example, notes that external forces seek to foment a "color revolution" in China, which would topple the CCP from power.[65]

CCP concerns are not only that outsiders might influence the broad Chinese population, but that senior political and military leaders might be suborned, undermining leadership morale and the will to fight. Events during the 1989 Tiananmen incident undoubtedly haunt Chinese decision makers about the possible impact of political warfare and other efforts to sow discord among senior leaders. As the senior Chinese leadership planned to use military force to suppress the protestors in Tiananmen Square, Major General Xu Qinxian, commander of the 38th Group Army, the centerpiece of ground forces in the Beijing Military Region, reportedly rejected the idea. He apparently felt that the protests "were a political problem and should be settled through negotiations, not force," a stance that reportedly led to his arrest.[66] Nor was Xu alone in holding such views. Other officers reportedly signed a petition to withdraw the troops. Eventually, other units had to be activated to move against the protestors. For China's leaders, the ability to control the military with absolute certainty was an open question.

Less than two years later, American and coalition forces overwhelmed Iraqi forces in Kuwait and Iraq. During Operation Desert Storm in 1991, Chinese commanders witnessed the impact of psychological warfare and public opinion warfare enhanced by modern technology. American and coalition forces coupled sustained aerial bombardment with leaflet drops and, in the Chinese view, carefully gauged the psychological impact of their attacks. The ferocity of initial strikes, moreover, had their own psychological impact, enhancing dedicated psychological warfare efforts.[67]

At the same time, Chinese analysts saw American and coalition forces waging public opinion warfare and psychological warfare campaigns to both undermine Iraqi support for Saddam Hussein and deny Iraq international support and sympathy. Chinese analysts have identified a variety of public opinion warfare techniques, ranging from spreading rumors via the media to describing Iraqi destruction of Kuwaiti oil fields as "environmental terrorism." All these measures denied Iraq any foreign sympathy, while eroding the regime's internal support.[68] The United States also employed monetary inducements and threats of war crime trials to undermine Iraqi military leaders' willingness to fight or otherwise obey Saddam's orders. Chinese writings assess that these political warfare efforts helped propel the American victory in the Gulf War by undermining Iraqi will.[69]

For China's leadership, the threat is clear: an advanced adversary, using various means of manipulating and inserting information, could create

divisions within the party's military, between military and civilian leaders, and between leadership and masses. The adversary could then exploit these divisions to erode national will, instill defeatism, and fray national support, thereby defeating the PRC.

This has made CCP efforts to control information and its flow both into and within China, in both wartime and peacetime, even more urgent. It has also made the CCP prioritize efforts to influence how that information might be perceived and interpreted. These include controlling the news, establishing an extensive web of Internet controls and censorship, as well as specific monitoring and control of social media.

Government Limitation of the Internet

While China's opening to the West forced it to accommodate greater media access, this was controllable. As described earlier, the Central Propaganda Department has long been an established mechanism for press censorship, so it could readily accommodate changes in the traditional media environment, including greater foreign presence. Indeed, even with the introduction of foreign journalists, there were still only a restricted number of outlets. The number of persons and entities that required monitoring remained limited. Previous media access controls (e.g., press passes, visas) remained sufficient to limit the newly expanded foreign press.

By contrast, the Internet poses an unprecedented threat to governmental ability to control information flow. This is in part because the CCP wants China to have broad access to the Internet. It is a key means of conducting business; China could not hope to participate in the modern global economy if it did not have ready connectivity with global information networks. It also easily accesses the global wealth of knowledge, an essential means for improving China at relatively low cost.

But access is a two-way street. Expanding linkage to the global information network raises the potential vulnerability of Chinese networks to significant criminal activity. China regularly argues that it is among the most-hacked nations in the world. In 2012, for example, the Chinese reported that 22,000 phishing websites had targeted Chinese netizens, while 14 million mainframes in China had been hijacked by various Trojan horses and botnets. Many of these are traced to foreign websites, "with the United States being the largest source of such hacking activities."[70]

Moreover, just as Chinese authorities use the Internet to obtain information and to influence others, other players, including both state and nonstate adversaries, can use it to transmit information to Chinese audiences. Senior Chinese leaders including Deng Xiaoping, Jiang Zemin, and Hu Jintao have all warned of Western efforts to subvert China through "Westernization" and

"peaceful evolution," that is, eroding CCP legitimacy (leading to "peaceful evolution" away from CCP rule). As one observer astutely notes, *the entire basis* of the past three decades of Chinese economic reform has been

> to benefit from Western technology and from trade with the global market economy *without* converging into the West's liberal democratic governance model.[71]

Chinese authorities consider efforts to draw China into that Western model, whether conscious or not, a de facto form of political warfare. The introduction of the Internet only exacerbates them.

If the Chinese leadership is going to prevent an opponent from effectively applying various forms of information against the population and leadership, it must be able to control information flow across the Internet. Indeed, because the whole purpose of the Internet is to disseminate information, it constitutes a major challenge to central government efforts to maintain control, even as it helps to stimulate Chinese economic development by facilitating information sharing and access. Consequently, substantial sums and effort have been invested in controlling potential adversary access to the Chinese population and senior military and civilian leadership. These efforts coincide with a broader interest in maintaining control over the Chinese population, given the omnipresent risk of unrest. Managing this threat to regime control has therefore entailed highest-level attention and a multilayered approach.

Highest Political Levels Are Involved

The importance of controlling the Internet, as noted earlier, has involved various senior leaders in a range of different entities. These organizational gyrations reflect changes in Chinese priorities, whether in terms of relative emphasis accorded "informationization" versus broader economic modernization efforts or information security relative to other aspects of fostering informationization. It is also a result of the challenges posed by the dynamic nature of the information environment, as information technology has rapidly evolved.

Xi Jinping appears to have concluded that information security and control of the Internet will be a central priority for his tenure (through 2022). In February 2014, the latest iteration of these efforts emerged, "the Central Internet Security and Informationization Leading [Small] Group." This group, according to the Chinese press, "is designed to lead and coordinate Internet security and informationization work among different sectors [of the Chinese government], as well as draft national strategies, development plans, and major policies in this field."[72] The group will develop comprehensive plans for policing cyber security, while promoting the broader use of information technology.

This leading small group is led by Xi Jinping himself, while Premier Li Keqiang and Liu Yunshan, both members of the Politburo Standing Committee, are his deputies, making the group the most senior ever established for informationization.[73] The official presence of three of the seven members of the Politburo Standing Committee reflects the priority accorded to its tasks.

Xi's remarks at the inaugural meeting of the group clearly expressed his concerns. Information security and informationization, he observed, were two aspects of a single whole, requiring unified planning, unified advancement, and unified implementation. Similarly, information security is an integral part of national security. "Without information security, there can be no national security."[74]

The General Office of the Central Internet Security and Informationization Leading Group is responsible for the day-to-day operations of the leading group, as well as preparing meetings, agenda setting, and so on. The director of that office therefore wields substantial authority in implementing Chinese policies on Internet security. Xi Jinping decided to appoint Lu Wei as the head of the general office. Significantly, Lu is also the head of the State Internet Information Office (SIIO), also known as the China Cyberspace Administration.

Lu's early career had largely been with the state-run Xinhua News Agency, where he had been bureau chief for Guangxi Province and later secretary-general and deputy director of the entire agency.[75] He then became vice mayor of Beijing (equivalent of being a vice governor) and head of Beijing's Municipal Propaganda Department. In 2013, he became the second head of the SIIO, which had been created by the State Council Information Office in May 2011, with responsibility for all Internet-related information activities. His career path paralleled his predecessor's at SIIO, Wang Chen. Wang had also risen through the ranks of the Chinese news media (although mainly *People's Daily,* rather than Xinhua). Both Wang and Lu therefore are intimately familiar with China's propaganda system and legacy information control organizations and procedures. As important, they had both long practiced controlling information flow.

By appointing Lu to this central position, Xi was making clear that Internet security would be closely enforced by state agencies, including the SIIO. When established, the SIIO was expected to streamline the various bureaucracies that oversaw the Chinese Internet. It was to "direct, coordinate, and supervise online content management, and handle administrative approval of businesses related to online news reporting," as well as "investigate and punish websites violating laws and regulations."[76] Senior SIIO members included a vice minister of public security, Zhang Xinfeng. The security role was sharpened when the State Council issued a circular in August 2014 announcing the

reauthorization of the SIIO. The circular noted that the SIIO's roles and responsibilities include the healthy and orderly development of the Internet, protection of the citizenry, and maintenance of national security and public interest.[77]

Current Internet Governance Is Challenged

One of the themes that Lu has repeatedly invoked, constituting the first layer of China's approach to protecting itself from the Internet, is the concept of Internet sovereignty. As Lu stated in 2014 at the World Economic Forum in Davos, "So we must have a public [international] order. And this public order cannot impact any particular local order."[78] Lu's comments reiterate Beijing's long-standing calls for extending national sovereignty across the Internet. For the Chinese leadership, only by altering the international Internet governance structure, revising underlying assumptions, and gaining acceptance of "Internet sovereignty" can China defend itself from Internet-borne threats to information control. By delegitimizing the free flow of information, Chinese authorities would justify efforts to control what information can flow across state boundaries and could even seek assistance from other states in constricting that flow.

From Beijing's perspective, determining who has a voice in managing the Internet is vital, as that can limit who can access the Internet. For the Chinese leadership, Internet governance is a reflection of national authority and power. The Chinese argue that Internet management should be limited to nation-states, reiterating this position in various official documents, such as the "2006–2020 National Strategy for Informationization Development" and the 2010 Chinese white paper on the Internet, as well as speeches by officials such as Lu Wei and Xi Jinping.

As important, the ability to authorize Internet names and addresses is also the ability to manage a strategic resource, since those names and addresses determine how one accesses the Internet (and how others access you). Given its importance, the ability to authorize Internet names and addresses cannot be left in the hands of foreigners.[79] Nor can it be lightly granted to nonstate actors who might challenge Beijing's authority.

There are a host of entities that the CCP has sought to mute and does not want to have unfettered access to the Internet. For example, it does not want to cede any kind of cyberspace naming authority to Taiwan. Indeed, one Chinese consideration about Internet governance is its desire to restrict the online voice of the authorities in Taipei, to ensure that they have no more prospect of international support in cyberspace than they do in the current political environment. As troubling for the CCP is the ability of groups such as the Tibetan government in exile or Falun Gong to voice adversarial positions and challenges to Beijing via the Internet.

This Chinese interest in preserving national sovereignty on the Internet, including maintaining control over how "China" is represented in cyberspace, has led to fundamental antagonism toward the current structure of Internet governance. When the Internet first began to grow beyond a handful of educational and governmental institutions, the United States vested its administration in the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit entity.

In order to reach a website, a computer user must enter an address in cyberspace. This address is a unique name or number (or combination). The ICANN staff administers the "domain name system" (DNS), which links the names of various websites, computers, and so on, with their numerical Internet protocol (IP) addresses. This includes authorizing and accrediting the highest-level lists of names, referred to as the "top-level domain" (gTLD) name registrars, who in turn can authorize other entities to grant names (and register them).[80] In essence, since its establishment in 1998, ICANN has had the authority to determine who can obtain the unique identifiers, or IP addresses, that allow others to access one's information on the World Wide Web.

ICANN policy has been grounded in the "multistakeholder" model. This system seats governments alongside other elements of global society, including academia, business, civil society (e.g., religions, nongovernmental organizations), and industry, managing the Internet as a whole through a consensus-based process. Individuals, as well as larger organized groups, are represented, none of them enjoying a privileged place at the table. The objective is to sustain the Internet as a borderless realm, where information flows freely.

Not surprisingly, the Chinese have opposed this multistakeholder approach, preferring a much more state-centered one. Ideally, from Beijing's perspective, Internet governance should be exercised primarily by governments, who would establish the rules for Internet activity, including the ability to apportion Internet addresses (and generally manage its activity) within their national borders. In short, state sovereignty would be extended to cyberspace. China objects to ICANN at a fundamental level—a state-centric governance model can hardly be managed by a nonstate actor, much less one that views other nonstate elements as coequals.

More practically, China has long had suspicions that ICANN is a creature of the United States. This has been exacerbated by ICANN's failure to accept Beijing as the sole legitimate voice for all Chinese-related entities—including Taiwan. The granting of a domain name (—.tw) to Taiwan implied that it was a separate entity, at least in cyberspace, from China (which has the domain name—.cn). The inclusion of Taiwan in the governmental committee (in effect treating it as a state) further alienated Beijing and resulted in Chinese boycotting of the ICANN "Governmental Advisory Committee" from 2001

to 2009.[81] Only when Taiwan's delegation was renamed as "Chinese Taipei" in 2009 did Beijing agree to send representatives to the committee.

Given these problems, the Chinese, as well as other authoritarian states such as Russia, have wanted to see Internet governance transferred from ICANN to the International Telecommunications Union (ITU), an agency of the United Nations. China formally proposed this at the 2005 UN-sponsored World Summit on the Information Society (WSIS). In September 2011, China and Russia, along with Tajikistan and Uzbekistan, submitted a proposal for an "International Code of Conduct on Information Security" to the UN Security Council that would enlarge the role of the ITU at the expense of ICANN.[82]

The submission was a clear attempt to shift Internet governance toward states. One clause, for example, sought to

> reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack, and sabotage.[83]

This clause would justify restrictions on any dissident groups that governments (including Beijing) assessed as threatening their "information space." It would also ensure that entities such as Taiwan would not have their own domain name, except in the unlikely event that the governing state (i.e., China) would agree. As the proposal also noted, governments were to "lead all elements of society . . . to understand their roles and responsibilities with regard to information security."[84] The state, in short, would have "policy authority for Internet-related public issues," eclipsing all other players, unlike in the multistakeholder model. (An updated version, although still holding largely to the same points, was subsequently submitted in January 2015 by the original four states, now joined by Kazakhstan and Kyrgyzstan.[85])

Meanwhile, Chinese authorities have sought to undermine the multistakeholder approach in other ways. There are five Regional Internet Registries (RIRs), which help in the assignment of IP addresses. The RIRs (one each for Africa, Asia, North and South America, and Europe) are private not-for-profit corporations, like ICANN. Within the Asia-Pacific Network Information Center (APNIC) purview are several National Internet Registries (NIRs), intended to address unique national requirements. These NIRs are also authorized to issue IP addresses and register names, like the RIRs and ICANN in general.

The Chinese NIR, the China Internet Network Information Center (CNNIC), however, has sought to control the issuance of addresses within China, pressing Chinese companies and Internet service providers (ISPs) to go through themselves, rather than through the APNIC. In 2004, Houlin Zhao, the then director of the ITU's Telecommunications Standardization Bureau, pushed for national authorities to manage the allocation of at least a portion of the new IPv6 (Internet protocol version 6) addresses, rather than relying on the RIRs.[86] Zhao, who has since risen to secretary-general of the ITU, acknowledges that he has a different vision for Internet governance, noting that ITU is often seen as pursuing a more top-down approach.[87]

Domestic Legal Controls on the Internet

In addition to seeking to modify the international Internet governance structure, the Chinese have been steadily creating a domestic legal and regulatory framework that firmly extends the state's grip over all parts of China's internal cyber community. This effort began almost as soon as China linked to the Internet, and even before commercial access was made available to the broader Chinese public. In February 1994, the State Council issued State Council Order 147, "Regulations for the Safety Protection of Computer Information Systems." This vested the Ministry of Public Security (MPS) with responsibility for supervising computer information in China.[88] This was further supplemented by State Council Order 195, issued in February 1996, which listed specific Internet governance regulations. Beijing has since issued an array of regulations, laws, and directives discouraging "inappropriate" use of the Internet and its information.

In December 1997, the MPS issued regulations for computer network use relating to preservation of social order and stability. These regulations included provisions that forbade individuals from using the Internet to jeopardize Chinese national security, to "harm the interests of the State, of society, or of a group" or to tamper with computer information networks and the data residing therein. The regulations also bar using the Internet to create, replicate, retrieve, or transmit information that:

- Incites resistance to the Chinese constitution, laws, or administrative regulations;
- Incites overthrow of the government or socialist system;
- Incites division of the country or harms national unification;
- Incites hatred or discrimination among nationalities or harms their unity;
- Distorts the truth, spreads rumors, or destroys social order;
- Promotes feudal superstitions, sexually suggestive material, gambling, violence, or murder;
- Furthers terrorism, incites others to criminal activity, or openly insults or slanders other people;

- Injures the reputation of state entities; or
- Promotes other activities that violate the constitution, laws, or administrative regulations.[89]

This range of prohibited activities encompasses such potential avenues for political warfare as advocating independence for Taiwan, Tibet, or Xinjiang; engaging in religious proselytization (which might destroy social order or promote "feudal superstition"); or criticizing elements of the government (injuring the reputation of state entities).

Three years later, the Chinese National People's Congress (NPC), the national legislature, issued the "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security." In the interests of "promoting what is beneficial and eliminating what is harmful," while preserving state security, the 2000 decision (effectively a law) delineated what constituted criminal activity in the realm of computer activities. As with previous regulations, the first section of the law again emphasized the importance of information security. It prohibited such acts as "invading the computer data system of State affairs, national defence [*sic*] buildup, or the sophisticated realms of science and technology," intentionally spreading computer viruses or otherwise adversely affecting the normal operations of the state's computer networks.

In addition, the decision made clear that criminal acts that threatened the security of the state or social stability were also punishable. Such acts included using computer networks:

1. To spread rumors, libels, or publicize or disseminate harmful information to whip up attempts to subvert state power, to overthrow the socialist system, or to split the country and undermine unification of the state;
2. To steal or divulge state secrets, intelligence, or military secrets;
3. To stir up ethnic hostility or discrimination and thereby undermining national unity; or
4. To form cult organizations or contact members of cult organizations and obstructing implementation of state laws and administrative regulations.[90]

Supplementing earlier MPS regulations, the NPC decision also dictates that using computer networks to violate the administration of public security even if it "does not constitute a crime shall be punished by the public security organ."[91]

Additional government policies supplement and refine Chinese information security policy by specifying standards and requirements for Chinese information security management and systems. In 2003, the "National Coordinating Small Group for Cyber and Information Security" promulgated "Document #27" (presumably denoting the 27th official document this group issued in 2003), formally entitled, "Views of the Leading Small Group Regarding the Strengthening of Information Security and Safeguarding Work." This document reportedly marked the first time that information security was explicitly incorporated into planning for economic development, social stability maintenance, safeguarding national security, and strengthening cultural development.[92]

The "Multi-Level Protection Scheme" (MLPS) was laid out in 2007 in the "Methods of Tiered Protection and Management of Information Security," or Document #43 of that year.[93] This was issued jointly by the Ministry of Public Security, the State Secrecy Bureau, the State Cryptography Administration, and the State Council Information Office. The MLPS reflects senior-level interest across multiple bureaucracies in ensuring that Chinese information security software remains firmly in the hands of Chinese-owned companies. According to the MLPS, a variety of governmental and nongovernment entities deemed central to national security or strategic interests can only use information security products that originate in China. These entities included banks, transportation, and energy firms, as well as state agencies associated with customs, commerce, telecommunications and broadcasting, or national security.[94] It now also includes Chinese ISP firms.

In 2010, the Chinese began to send inspectors to the field to verify compliance with the MLPS. Non-Chinese firms such as Microsoft reportedly have had their access to the Chinese market extremely curtailed. The restrictions on outside access may have been motivated in part by the desire to create a protected market for China's information security firms, but it also restricted a potential line of vulnerability by limiting foreign ability to reach Chinese computers.[95] In 2012, the State Council issued "Several State Council Views on Emphasizing and Pushing Informationization Development and Realizing the Safeguarding of Information Security" (also referred to as "Document #23"). This document again emphasized the need to strengthen information and network security, especially for government information systems.[96]

Chinese efforts to restrict foreign access likely gained impetus after the 2013 revelations about American cyberespionage by Edward Snowden. In 2014, the Chinese government reportedly excluded foreign antivirus companies Symantec and Kaspersky from bidding on Chinese government contracts.[97]

Central government efforts to control information flow are not solely aimed at users. ISPs, cybercafes, and other access providers are also closely scrutinized. The State Council has issued various regulations to govern online businesses. ISPs and Internet content providers (ICPs) were licensed by the

Ministry of Information Industry (MII), and now by the Ministry of Industry and Information Technology (MIIT), which absorbed MII in 2008. ISPs are also expected to adhere to the "Public Pledge on Self-Discipline for China's Internet Industry" and are "encouraged" to join the Internet Society of China, a governmentally backed "nongovernmental organization," which disseminates the latest guidelines on censored topics, terms, and so on.[98]

These entities and pledges help promote "self-regulation." Private companies such as ISPs are expected to enforce legal requirements, whether use of Chinese software for information security or monitoring their own traffic and networks for dangerous or malicious behavior. ISPs, cybercafes, and other providers are responsible for ensuring that all users register with their real names, a centerpiece of many Chinese efforts to limit anonymity on the Chinese Internet. At the same time, as will be discussed later in this chapter, ISPs are also part of the human censor network that backstops technical censorship methods.

As cybersecurity is more explicitly linked to national security, pressure on these companies will grow. Article 25 of the 2015 Chinese National Security Law specifies that the state's national security responsibilities include maintaining national network and information security, stopping "unlawful and criminal activity," including "dissemination of unlawful and harmful information," as well as "maintaining cyberspace sovereignty, security, and development interests." It specifically includes national security reviews and oversight management of "Internet information technology products and services."[99] The censors employed by many ISPs and other cyber companies are kept busy by these requirements.

Meanwhile, the Chinese cybersecurity law that came into effect on January 1, 2016, will further complicate matters. This legislation will not require foreign companies to keep local user data in China and did not require installation of government-accessible backdoors in software (as had been proposed in earlier drafts). It *does* require all telecommunications and Internet companies doing business in China to cooperate with Chinese law enforcement and security organizations. This includes controlling information flow in defense of cyberspace sovereignty, as well as information network security and development efforts. The legislation requires all companies to provide "technical assistance," including decryption of user data, in support of "counterterrorist" activities.[100]

Technological Means of Limiting Access

While Chinese diplomats strive to extend national sovereignty to cyberspace and Chinese legislators and party officials design legal controls over domestic Internet behavior, Chinese engineers have sought to technologically limit and monitor data flowing into China. This is facilitated by Beijing's limiting connections to the broader global information networks

(and therefore global access into China). Fiber-optic cables enter China at only three points—the Beijing–Tianjin region; Shanghai; and Guangzhou. There are only a limited number of Internet exchange points (IXPs) running via these cables, most controlled by the Chinese government. This leads to congestion and a slower Internet speed for Chinese users accessing the outside world but eases the government's ability to monitor traffic entering and leaving China.

As important, the Chinese government has long supported research in additional programs and measures that limit information flow. The 2000 decision on preserving computer network security charges the government at all levels to "support research and development of the technology for computer network security and enhance the ability of maintaining security of the network."[101] A high priority has been filtering foreign content, in terms of not only what outsiders can send into China but also what Chinese netizens can access.

A centerpiece of this effort is the "Great Firewall of China" (GFWC). This "on-path" system is the first line of technical defense, monitoring traffic across the three portals that link the Chinese portion of the Internet to the rest of the world. It also has some capacity to monitor internal Chinese computer activity, although this is sometimes conflated with the "Golden Shield" project, which is more focused on monitoring domestic Chinese online behavior. The avowed purpose of the GFWC is to keep outsiders from being able to attack Chinese Internet users. In reality, the GFWC has demonstrated an ability to censor websites and even individual web pages and images, limiting Chinese citizens' ability to access the global Internet. Theoretically, the GFWC could shut down connectivity between China and the rest of the global Internet entirely, if necessary.

The GFWC employs a variety of methods to prevent Chinese netizens from accessing information that might contradict or challenge the government's preferred line. IP addresses may be blocked, or attempts to connect to them may be misdirected. In addition, in a different application of typical intrusion detection systems, the GFWC undertakes data inspection and filtering to examine uniform resource locators (URLs), or web addresses, as well as the numeric IP addresses. It can also examine actual content, in order to more precisely filter out individual web pages and images.

The GFWC's purpose is not simply to block content and limit access to forbidden sites; it also seeks to make such content and access more complicated and frustrating, so that users will avoid them. Thus, the GFWC typically tries to limit the degree to which its censorship is noticeable to the average user. While the GFWC will block access to some websites (or even individual pages or images), it does not necessarily interfere with access to other parts of the Internet. A user may therefore not realize that his or her search has been blocked but may instead assume that a website is no longer operating or is being modified.

The GFWC is meant to complement various other measures, such as real-name registration and human censors, as well as broader laws and pronouncements regarding unacceptable or dangerous behavior (not just online), to discourage efforts to access forbidden information. It is estimated, for example, that less than 10 percent of China's netizens engage in political discourse on the Internet at all.[102] Although this remains an enormous number (since China has over 500 million users), this makes censorship and information control more manageable.

HOW THE GREAT FIREWALL OF CHINA WORKS

For a Chinese user seeking to access a foreign website, his or her computer must connect with a domain name server (DNS), which will seek out the desired Internet protocol (IP) address. The IP address is the unique 32-digit (in IPv4) or 128-digit (in IPv6) "location" on the Internet.

The DNS server, in turn, will either provide the address or query other authoritative name servers for the desired location of the specific IP address. This information will then be transmitted to the Chinese user's computer. A query may have to travel through several layers of domestic servers to reach one of the three international exchange points (the portals where China's Internet links to the broader, global structure).

In China, authoritative name servers and DNS servers are run by either Chinese companies or the government. As such, they are incorporated into the Internet filtering process that constitutes the Great Firewall of China (GFWC). These filters employ similar software to security firewall programs. But where other firewalls are designed to detect malicious software and efforts to infect computers, the GFWC is intended to detect and halt dangerous ideas and information.

The GFWC is also different from most firewall systems because it is an *on-path* system. Most firewalls are an "*in-path* barrier between two networks: all traffic between the networks must flow through the firewall."[103] The GFWC, on the other hand, "mirrors" inbound and outbound data packets to what are believed to be separate clusters of government-run computers, reassembling the data to some extent, in order to examine their destinations and even their content. The GFWC then employs several methods to keep China's population insulated from potentially dangerous information.

- *Blocking IP addresses.* One of the most basic methods for the GFWC to limit access is to prevent a user's computer from connecting to a given IP address. The GFWC retains a list of banned IP addresses. When a user seeks to connect with one of these at a foreign server, the GFWC refuses to allow it through the intervening connections.

  The social media site Facebook, for example, has a website, facebook.com, which is located at a given IP address, which is known and fixed. Any effort to connect to that address will be broken automatically by the GFWC. This is similar to how parental controls work and is common to many commercial firewall programs.

- *Misdirecting IP addresses.* This is also known as "DNS poisoning." In some cases, the Chinese may not forbid access to a given IP address but may misdirect a connection attempt instead. In order for a query to reach its destination, it must have a proper address. Thus, the DNS and authoritative name servers are expected to have up-to-date address lists in order to route messages to their proper destination. With the GFWC, however, China's various name servers will either withhold an answer when queried or give an incorrect answer. The querying computer will be directed to a different website's IP address or to a warning page (e.g., a page stating that the query is into a sensitive area).
- *Data inspection and filtering.* This is also known as "deep packet filtering." The Chinese authorities not only examine requests to connect (which typically require one data packet) but also the responses, by reassembling response packets. Thus, in many cases the GFWC can examine the contents of web pages and block pages based on that content rather than the IP address. Similarly, in some cases the GFWC has been even more precise, filtering out certain web pages or certain images, rather than blocking an entire website. The GFWC has also demonstrated that it can censor pages based on URLs or address name if it contains forbidden terms, such as "Falun Gong," the banned religious movement (which the Chinese characterize as a cult).

While the GFWC may sometimes simply prevent a connection between a Chinese requesting computer and a foreign website, at other times, it may disrupt the connectivity through other means. Some of these methods involve the transmission control protocol (TCP). Whereas the IP deals with data packets, the TCP essentially is the means by which programs exchange those data packets and establish network conversations. The TCP, in conjunction with the IP, defines how computers will communicate with each other (hence the commonly used abbreviation TCP/IP).

When a banned IP address is requested, the GFWC will sometimes drop the request (blocking the address) and substitute a series of false "TCP Reset" packets. The GFWC essentially informs the requester and the destination computer that the request could not be completed or was in error. By indicating to requester and destination that he or she has "dialed a wrong number," the GFWC causes the request to be rejected, breaking the connection. If the user persists in making the same request, the GFCW automatically blocks him or her and may do so for up to an hour.

Another TCP-related method for disrupting communications is for the GFWC to send data packets (which it has already intercepted) to the foreign-sourced website out of sequence. The foreign site, receiving requests that appear to be out of order, then cannot synchronize valid server requests that are arriving at the same time as the invalid (i.e., out of sequence) requests from the GFWC.

Not surprisingly, a number of efforts have emerged to try to circumvent the GFWC, which in turn have led to Chinese government countercountermeasures. For example, Chinese and foreign computer users have tried to foster "virtual private networks" (VPNs) to allow less fettered access to the global Internet. VPNs establish secure connections between a user's computer and

a separate network, so that the user's computer is treated as though it were part of that local network (even if it is physically separated). One can then access any information that the local network might contain.

VPNs are often set up by large companies to allow widely separated locations to share files and access each other's data. Through "tunneling protocols," they can establish secure links even in the face of blockages, such as those imposed by the GFWC. VPNs have been of particular interest to foreign companies that have subsidiaries in China; establishing a VPN can help make internal communications more secure.

A VPN not only allows sharing data that resides on the network but also allows users access to anything that the network can "see." For Chinese users, a VPN provides a potential link to the broader Internet outside China. By joining a commercial VPN provider, they can link to that provider's network located outside China, which would then provide access to Google, Facebook, and other sites that are currently blocked by the GFWC.

Chinese authorities began to develop tools to crack down on the use of VPN as soon as they began to gain popularity. Some commercial VPN sites were entirely blocked. Another counter to established VPN connections was emplaced in 2012, with updates to the GFWC allowing it to "learn, discover, and block VPN protocols automatically."[104] It is believed that, through "deep packet inspection," the GFWC can at least determine whether packets are encrypted, even if their content remains inaccessible to the censors. If a substantial amount of encrypted traffic is detected bound for a particular network, the GFWC may then block that path.

By 2014, commercial VPN companies that serve Chinese clients reported even more extensive interference with their services.[105] Whereas earlier versions had blocked OpenVPN, the least sophisticated tunneling protocol, further upgrades to the GFWC are now apparently affecting more advanced tunneling protocols, such as PPTP (Point-to-Point Tunneling Protocol) and SSh2 (Secure Shell-2), making it ever harder to establish and maintain VPN connections through the GFWC.

Supplementing the GFWC is the additional layer of surveillance imposed by the "Golden Shield" project. Managed by the Ministry of Public Security, this is a nationwide digital surveillance network that correlates Chinese citizens' online behavior with information obtained via other means such as telephone monitoring and closed circuit television feeds, citizen tax data, and purchasing habits (derived from monitoring credit card use and other electronic monetary transfers). The goal is to provide both local and national authorities with a complete profile on any persons of interest.

The GFWC, supported by human censors, operates at the network level. The Chinese authorities, however, have also sought to extend their reach to the level of individual computers. In 2009, the Chinese leadership attempted

to require the installation of "Green Dam" software on all computers sold in China. The program would use a combination of image recognition technology and text filtering to limit access to "vulgar" sites and images. While ostensibly intended to protect children from pornography and other adult sites, according to one study, "Green Dam" software would in fact block access to religious and political sites. More important, it would embed itself deep within the computer's operating system and actively monitor "individual computer behavior, such that a wide range of programs including word processing and email can be suddenly terminated if content algorithm detects inappropriate speech."[106] This would have effectively extended Chinese censorship to individual computers and affected many programs that were beyond the reach of the GFWC. For example, Green Dam could prevent users from accessing or transferring information via CDs, DVDs, or flash drives/memory sticks by stopping the computer from reading such media.

The requirement that all personal computers sold in China incorporate this software was extremely controversial, and even Chinese state media questioned the viability of this program (including whether it would be reliable or would interfere with other programs).[107] The decision was eventually rescinded, but the concept is indicative of Chinese officials' desire to technologically control and constrain access to information.

Human Censors Supplement Censorship Efforts

In addition to the automated censorship of the GFWC and the "big data"–based surveillance provided by the "Golden Shield," there is a human element in Chinese efforts to control the Internet. Those Chinese citizens who wish to circumvent the Golden Shield of domestic Internet surveillance, as well as the GFWC, have shown a facility in finding ways to bypass the automated censor systems. Discussions of the Tiananmen massacre, which occurred on June 4, 1989, for example, have sometimes included references to May 35th, April 65th, and March 96th.[108] By avoiding specific reference to "six-four," that is, June 4th, such references could avoid detection by the algorithms put in place.

Such efforts are facilitated by the plethora of homophones in Chinese. An entire lexicon of such terms has emerged, including "river crab" (a homophone for "harmony," a long-standing CCP-touted virtue) and "grass mud horse" (a homophone for a crude sexual act involving one's mother), as Chinese netizens express unhappiness with various policies or lampoon government figures.

Moreover, global developments can create subversive concepts and memes more rapidly than automated algorithms can adjust. When the Arab Spring exploded in 2011, the government was forced to rapidly censor terms such as "jasmine," a symbol used by various Middle East protestors.

Recognizing that human ingenuity, coupled with current events, is likely to outpace automated search systems' ability to curtail dissemination of forbidden information, the Chinese authorities have created a network of human censors to further enforce restrictions.

The human censorship effort relies heavily on the ISPs. Because the Chinese government holds to the position of "intermediary liability," that is, "one is responsible for what one publishes," Chinese ISPs are incentivized to limit potential posting or discussion of forbidden topics.[109] As a result, not only have most ISPs installed various filtering systems to detect (and eliminate) sensitive words and phrases, but they also field teams of employees and volunteers who monitor chat rooms, review blogs and web pages, and otherwise help ensure that what is published via the ISP does not trouble the authorities.[110]

These, in turn, are supported by the government's own cyber police. In 2004, this was estimated to already number some 30,000 members.[111] A decade later, reports suggest that China may have 100,000 to two million government censors, tracking both Internet and social media (including microblog) posts and comments.[112]

Government Control of Social Media

The rise of social media poses an additional problem for Chinese efforts to control information flow and dissemination. The proliferation of video and photos further expanded the forms of information now available, while enhancing its credibility. Indeed, social media have become a major part of the Chinese information environment, as much of China's netizenry accesses the Internet via mobile phones and social media platforms. Chinese microblogging sites such as Sina Weibo, Sohu, and Tencent, the PRC counterparts to Twitter, have 200 million subscribers.[113] They are the "primary space for Chinese netizens to voice opinion or discuss taboo subjects."[114] Not surprisingly, this has led to a range of additional controls on information dissemination.

In 1999, China reorganized its telecommunications organization and began to offer cell phone services. By 2004, Chinese were opening up five million new cell phone lines every month, totaling some 350 million cell phone users by the next year.[115]

The proliferation of cell phones allowed China to rapidly modernize and expand its communications networks, without having to invest massively in physical (copper or fiber-optic) telephone lines. At the same time, it also created a new form of connectivity, through text messages. Chinese cell phone users transmitted some 200 billion text messages (SMS, or "short message service") in 2003, averaging 651 per user, at a rate of nearly 7,000 per second.[116] For Chinese authorities, the introduction and rapid proliferation of

cell phones, and the consequent ability to employ text messaging, constituted a major new challenge to controlling information flow.

Indeed, even as this new communications form was taking off, Chinese authorities realized that it constituted a major threat to the state's monopoly on information and its dissemination. This was highlighted by the 2002–2003 severe acute respiratory syndrome (SARS) crisis in China. "While China's government-controlled media was prohibited from reporting on the warning, the news circulated via mobile phones, e-mail, and the Internet."[117] Information propagated far faster than central authorities intended—which meant rumors and misinformation spread rapidly as well. Public confidence in the government rapidly eroded, exacerbated when Dr Jiang Yanyong, a retired military surgeon, e-mailed two Chinese TV stations that the Chinese health minister was lying when the latter declared SARS was under control in the PRC. While the Chinese news media did not report on Dr Jiang's comments, his views were reported in the foreign press, from which it rapidly disseminated back within China.

Although the PRC eventually got SARS under control, central authorities now recognized that social media and cell phones constituted a major threat to governmental information control. This led to several efforts to reestablish tight control over these new forms of information dissemination. By July 2004, barely four months after Dr Jiang's e-mail, Chinese authorities were already policing the cell phone system, fining and shutting down cell phone providers who were not monitoring text messages passing over their systems.[118]

The Chinese leadership appears even more worried about how social media had been exploited by forces for political and social change abroad. Beginning with the "Rose Revolution" in Georgia in 2003, and the subsequent 2004 Ukrainian "Orange Revolution" and 2005 Kyrgyz "Tulip [or Pink] Revolution," a number of former Soviet republics underwent political upheaval. In all of these "color revolutions," popular forces demanded democracy and more representative government. Other protests rocked Serbia and Lebanon. Many protests in these countries were organized through social media such as e-mails and text messages. This new form of communications allowed organizers to address large groups simultaneously, a vital tool for rapidly creating demonstrations and other public challenges to regime authority.

By contrast, governmental crackdowns in the face of public protests were often ineffectual, since governments in Cairo and Tunis could not control the social media networks that protestors were exploiting. Companies such as Twitter and Facebook were based abroad, and not vulnerable to local pressure. Moreover, governments could not cut off access to social media without also affecting their own connectivity to the global Internet.

To stem such possibilities, the Chinese have extended the comprehensive array of countermeasures against the free flow of information to various social

media networks. Rather than eliminating all social media, as in North Korea, the Chinese leadership has redirected the public's access to domestic companies, excluding foreign platforms.

The Chinese control of popular access to social media was amply demonstrated in 2009, as wholesale restrictions were placed on YouTube access. While only individual YouTube videos had previously been blocked, the Chinese now claimed that the service had posted fake videos of monks being beaten in Lhasa, Tibet, and therefore was undermining Chinese internal security.[119] Since then, the government has largely restricted access to YouTube; other foreign social media sites were soon similarly excluded from the Chinese market.

The Chinese authorities did not try to deny the Chinese people the benefits of social media, such as video sharing, however. Instead, they channeled popular demand for social media and attendant opportunities for information exchange and access toward domestic companies, programs, and platforms. Even as the GFWC blocked access to foreign social media programs such as Facebook and YouTube, domestic counterparts were allowed to rise in their stead. Initial efforts at such "electronic import substitution" began in the late 1990s and had begun to bear fruit by 2000. Just as China's physical information networks would be built from Chinese equipment, China's appetite for social media would be met by Chinese companies.

Today, Chinese computer users search the Internet with Baidu, instead of Google. They share videos through Youku, rather than YouTube, and they don't Tweet but microblog across Sina Weibo and Tencent. Chinese online shoppers browse Taobao and pay with Alipay. All of these products and platforms are managed by Chinese companies, and while the companies may not be state owned, they clearly cooperate with censors and submit to broader government control, much like the commercial news media in China. Indeed, as Weibo's public filings at the time of its initial public offering (IPO) noted, failure to comply with government demands for censorship "may subject us to liabilities and penalties and may even result in the temporary blockage or complete shutdown of our online operations."[120] Consequently, should the Chinese public try to organize themselves as Middle East populations did during the 2009 Iranian Green Movement, 2010 "Jasmine Revolution," and 2011 "Arab Spring," the Chinese authorities have the ability to mute and neutralize such efforts.

The Chinese response to various critical incidents has demonstrated these capabilities. In 2008, riots in Tibet led to restrictions on local Internet access and text messaging. Greater restrictions were imposed on Xinjiang after ethnic unrest turned deadly in July 2009. The government claims some 200 died and nearly 1,400 were injured in various riots and demonstrations.[121] Officially, the Chinese government stated that the "terrorists used the Internet and SMS messaging."[122] Chinese authorities promptly shut down all Internet and mobile text messaging in the region, yet maintained cell phone connectivity. This separation of functions had been engineered into Chinese telecommunications networks.

This nearly total information blockade lasted for several months, and it was not until the following May that full Internet and SMS was resumed. Subsequent Uighur-related incidents, however, such as the 2013 attack in Tiananmen Square, the 2013 outbreak of rioting in Turpan Prefecture, Xinjiang, and 2014 incidents in Kashgar Prefecture, Xinjiang, led to the prompt reinstitution of these information blackouts.

Tight controls on social media are not only imposed due to ethnic unrest, however. In 2012, when Chongqing party secretary Bo Xilai was rumored to be organizing a coup attempt against the central government, Chinese media companies Tencent Holdings (which manages QQ and WeChat) and Sina Corporation (which manages Weibo) both shut down their commenting functions to limit any discussion.[123] In November 2014, when the U.S. embassy in Beijing began providing regular readings of air pollution on its grounds, often contradicting official claims of clear skies and clean air, Chinese smartphones stopped linking to that information.[124]

More seriously, in 2014, Hong Kong residents protested when Chinese authorities appeared to be reneging on their pledge to allow universal suffrage in local elections. Beijing chose to interpret Hong Kong's Basic Law (the local equivalent of the Constitution) as allowing the people of Hong Kong to vote for their local government, *but* allowing Beijing the ability to determine who could qualify as a candidate for those votes. The result was the "Occupy Central" movement, as students and civic leaders protested Beijing's decision.

This, in turn, led to widespread censorship of news about Hong Kong on Chinese social networks and further restrictions on access to foreign programs and apps. Instagram, the Android-based photo-sharing system for cell phones, was suddenly inaccessible in China. At the same time, Sina Weibo's microblog and Tencent's WeChat began to delete references to Hong Kong demonstrations and Occupy Central gatherings.[125]

Such draconian steps of openly shutting down parts of the social media infrastructure seem to be invoked primarily in crises. For day-to-day oversight, Chinese authorities rely more on an overlapping array of measures that are less overtly intrusive but that shape and mold users' experiences. Much of this is implemented by social media sites, rather than the government per se. On Sina Weibo, one of the main Chinese microblogging sites (comparable to Twitter), this array of mechanisms includes prophylactic, near-real-time, and retroactive measures.[126]

For Sina Weibo users, many search terms are simply not accessible via that platform. The company maintains a list of search terms that is prohibited for all users, which means that information flow across Sina Weibo is constrained

from the outset. It is not clear as to who determines which terms are off-limits, although the Central Propaganda Department almost certainly plays a major role, in conjunction with service providers and various other government agencies.

As with Internet censorship, social media are then subjected to an array of additional controls, complicating and frustrating attempts to propagate dangerous or forbidden information. Subscribers who seek to post comments on sensitive topics (which change in light of broader news, social, and political developments) are subjected to an array of near-real-time measures. These can take effect within minutes of items being posted. One test saw some items deleted within 8 minutes, and one-third of questionable content deleted within 30. Over 90 percent had been deleted within 24 hours.[127]

Some of the measures include:

- *Explicit filtering.* If a Weibo user tries to post comments that touch on sensitive topics or content, he or she receives a message warning that the content violates Weibo's rules or government rules.
- *Concealing or camouflaging posts.* Weibo will appear to post items, so that only the posting user, but no one else, will see it. No indication is given to the posting user that the message has not gone to a wider audience.
- *Implicit filtering.* Weibo employs its own group of censors, with one senior company official acknowledging at least 100, but other reports suggesting as many as 700.[128] These censors will apparently manually check some items; users posting items that are being examined may be informed that a review is under way. Some of the posts are eventually posted, while others are not.

The implicit filtering approach is striking, since it indicates that a significant part of Chinese social media censorship still relies on human intervention. Chinese willingness to devote significant manpower to such a task (e.g., to monitor even a fraction of the billions of microblog comments a year) reflects the seriousness with which the government views social media oversight and censorship.

To ease the burden and make more efficient use of their censors, Chinese social media companies try to exploit the larger pool of subscribers to help police their information flow. Since May 2012, for example, Sina Weibo has offered "user credit" points to community members who report sensitive, inappropriate, or rumor-based postings to administrators. This, in effect, alleviates the pressure on full-time censors by adding tens of thousands of additional informal watchdogs, who can then cue formal censors for specific action.

These steps may be undertaken in conjunction with the imposition of additional restrictions on users. Some users, especially ones who often raise

sensitive or censored topics, are subjected to additional review of their comments and posts. It is not clear, though, as to whether this is a policy or is imposed episodically. In some cases, a user may even be dropped entirely. During one analysis, nearly 10 percent of 3,500 observed user accounts were closed over two months (although not necessarily for political or even censorship reasons).[129]

These near-real-time filtering measures allow Sina Weibo and presumably comparable ones at other Chinese social media platforms, to restrict the flow of information on key subjects and terms, and to limit certain posters' impact. In addition, there are supplemental procedures in place to further constrain the flow of undesirable information that might leak through. Posted items are subsequent reviewed and removed if necessary. Such retroactive measures include "backward keyword search" and "backward reposts search."

Backward Keyword Search

Sina Weibo censors apparently regularly review messages to see if they contain words or phrases that had not been recognized as sensitive when posted. Because the Chinese language contains many homophones, posters can employ various phrases and characters that might not, in and of themselves, trigger deletion by automated programs but which a human would recognize. This is an updated computer version of a long-standing form of protest in China. In the days before Tiananmen, for example, some people deliberately broke small glass bottles in public spaces because Deng's given name, "Xiaoping," is a homophone for "little bottle." Thus, protestors were "breaking Deng" by breaking bottles.[130]

Researchers examining Weibo post deletions found that many posts that contained a newly restricted phrase (e.g., a homophone for "celestial empire" (*tianchao*; 天朝), itself a phrase intended to reference the government) were deleted. These deletions were made not only on the day the phrase was discovered (or recognized as derogatory) but from earlier days as well. In essence, those earlier posts were removed from the records so that no search would detect them. Another example noted that posts from two to five days preceding a decision to censor a given phrase were all removed, often within five minutes of each other. "Those 44 posts are from different users, have no common parent posts, and have no common pictures. The only plausible explanation for this concentrated deletion would appear to be a keyword-based deletion."[131]

Backward Reposts Search

According to several studies, not only are individual posts deleted when they touch on sensitive topics or terms, but *associated* posts are often also deleted as well. This occurs within a remarkably short time; "in our deleted posts

dataset over 82% of reposted posts have a standard deviation of less than 5 minutes for deletion time."[132] This means that, like in Oceania in George Orwell's *1984*, not only are certain items deleted from the record, but all reference and associated posts are deleted as well, in effect creating "uninformation." This makes it much more difficult, if not impossible, to detect that such a post had ever existed.

For the Chinese leadership, the ability to monitor information and control its flow is an essential prerequisite for waging informationized warfare. It is the foundation for establishing information dominance and involves both offensive and defensive actions. Offensive actions include political warfare measures to define and influence how others perceive events, personalities, and positions. Defensive efforts justify enormous expenditure of human and financial capital, as they prevent adversaries from exploiting a major vulnerability.

4 Chapter

Information Warfare: Waging Information Campaigns in the Next War

While informationized warfare applies information to all aspects of modern warfare, and extends the concept of warfare to such arenas as the legal and public opinion realms, the PLA will also engage in "information warfare" (*xinxi zhan;* 信息战). This is the struggle for information dominance within the more traditional military arena. Indeed, some Chinese analyses conclude that information warfare is the main operational form of informationized warfare, directly affecting all other combat activities and goals.[1]

Information warfare entails specific efforts by the PLA to secure information dominance over the adversary's military forces. This emphasis on information dominance arose as the military gained greater exposure to joint operations, which the PLA has assessed as central to future wars. Indeed, information is intimately linked to China's understanding of joint operations, which will be a central part of fighting and winning future "local wars under informationized conditions."

The PLA's conception of joint operations has shifted from multiple, individual services operating together in a coordinated fashion in the same physical space to unified operations under a single command-and-control network. This focal shift corresponds to a comparable shift in the assessed importance of information. According to PLA analyses, successfully conducting joint operations at the campaign level elevates information's role to the same level as forces, time, and physical space as key, objective factors. Information is how participating forces relate to each other, as well as to time and space.[2]

GROWING EMPHASIS ON JOINT OPERATIONS

As noted in Chapter 2 ("Not Your Father's PLA"), the PLA began to focus on joint operations beginning in the mid-1990s, and codified this growing