Information War and Rethinking Phase 0

R Bebber

United States Cyber Command
Ft. Meade, Maryland
E-Mail: jbebber@gmail.com

Abstract: *In the Department of Defense, both military and civilian planners use a framework that divides military operations into six distinct phases. This type of framework may no longer have the utility it once enjoyed. This shift has less to do with technology changing the nature of war and more to do with how the United States differs from its adversaries in its understanding of war. Adversaries of the U.S. understand the state of the world to be one of conflict and competition and look to strategy to impose order through hierarchy. This article considers the Russian and Chinese approaches to the use of information in war and makes recommendations on how the U.S. might respond.*

Keywords: *Information War, Information Operations, Cyberspace, Phase 0*

Introduction

In the Department of Defense, both military and civilian planners use a framework that divides military operations into six distinct phases. These include: Shape, Deter, Seize the Initiative, Dominate, Stabilize, Enable Civilian Authority, and finally back to Shape. While perhaps having some utility at the operational and tactical level, this type of framework constrains strategic military planning. This constraint has less to do with technology changing the nature of war (it does not) and more to do with how the U.S. and its adversaries differ in understanding war and the role of information. Adversaries understand the state of the world to be one of conflict and competition and look to strategy to impose order through hierarchy. The American perspective is one that *peace is the norm* and *war is an aberration*. The emphasis of military planning is to return, as quickly as possible and with a minimal loss of life and property, to the steady state of the Shape phase, while achieving military objectives. Phase 0 is not seen as a state of conflict between the United States and other powers. Yet it is here, in Phase 0, that adversaries are conducting military operations designed to deter and ultimately defeat the United States, whether in cyberspace or in the broader "informationization" of warfare. It is an era of persistent conflict.

Information is the coin of the realm in this context. It is the resource to be harvested and used to provide competitive advantage. Russia's doctrine of 'hybrid warfare' relies on information control as a weapon, supported by clandestine destabilization operations and the maneuver of conventional forces. Chinese military writing argues that war has entered an era of "informationized operations," and the victor is the side which best gathers and uses information while denying it to the adversary (McReynolds *et. al* 2015). Islamic terrorist organizations use information resources for propaganda, recruitment, mentoring, command and control of forces, and the promotion of 'do-it-yourself' terrorism worldwide–a form of *iTerrorism*.

Cyberspace operations and cyber power permit states and non-state actors to act in the information space and through the information space to affect the physical world in diverse and important ways. The scale has grown dramatically, and even small groups or states can have an outsized effect. The American concept of Phase 0 is challenged as actors in cyberspace conduct activities that many would consider belligerent, if not direct acts of war. Some have suggested that Iran was behind the 2012 use of the *Shamoon* malware to attack the Saudi Aramco energy company, which destroyed the data on 30,000 hard drives (Infosecurity 2014). In 2014, it is believed that North Korea sanctioned a cyber-attack on Sony Motion Picture Entertainment in response to the release of the movie *The interview* (Sanger & Perlroth 2014) The Russian government is suspected of having conducted a recent cyber-attack on the Ukrainian power grid that cut power in 103 cities and towns (Perez 2016). The U.S. appears to have been the victim of cyber-attacks on its own power grid from Iranian and Russian actors (Burke & Fahey 2015). One common thread in all these examples is that, due to the difficulties in attribution, all actors suspected can plausibly deny they conducted these acts. The onus of whether to escalate or respond falls on the victim, likely encouraging future mischief. If these few examples of attacks were conducted by traditional military means, especially against civilian targets, there would be little doubt of how the U.S. would act. But the fact that these acts were conducted via cyberspace appears to have left security and military planners in a quandary about how, or if, the U.S. should respond.

In this era of "persistent conflict" (Casey 2008) *position* and *posture* must become the critical elements in shaping adversary perceptions on the willingness and capability of the U.S. to respond. A 'rebalance' or shifting of forces from one theater to another, as was presupposed by the U.S. rebalance to Asia is insufficient. Rather, it is about the ability to build and stockpile all elements of power, and to be capable and willing to use them. Technology provides unique capabilities and efficiencies to acquire that position and gain the 'information high ground'. The United States will need to rethink both the planning emphasis and how Phase 0 is approached. Phase 0 becomes the most important. The U.S. will have to think in terms of 'winning' in Phase 0 and will have to construct concomitant theories of victory here, because that is where the war is being waged.

The Environment of Persistent Conflict

The search for and use of information has always been a part of conflict and war. In verse 13 of the Biblical book of Numbers, God directs Moses to "Send men to spy out the land of Canaan, which I am giving to the people of Israel". In addition, the Mongols were noteworthy in their use of psychological warfare and deception to encourage enemies to surrender without fighting. And Ancient Egyptian Pharaohs would boast of their deeds and proclaim their divine lineage in hieroglyphic carvings on temples and monuments to promote the legitimacy of their rule. Today, however, the availability of information, as well as the means to acquire it and use it, far exceed any other point in recorded history.

Today's world might be described as the 'World of Moore and Metcalfe'. In 1965, Gordon E. Moore, co-founder of Intel, observed that the number of transistors in an integrated circuit doubled every year (later revised to every two years). Integrated circuits are arguably the backbone of the information technology revolution that Moore helped usher in, revolutionizing electronics, computers, automobiles, mobile phones, and home appliances. Exponential growth

in the number of transistors—for example, processing power—has powered growth in the amount of data, economic productivity, technology, and social change, since the late 20th century (Grothaus 2016). This growth would not have been possible without the concurrent decline in the cost of computing and data storage. The following figures reported in April 2016 by the Strategic Initiatives Group (SIG) illustrate this growth:

- More data now crosses the Internet every second than were stored in the entire Internet 20 years ago;
- Every two days, people create as much information as we did from the beginning of time up to 2003. In 2012, 90% of all the data that existed in our entire history had been created in the previous two years. By 2020, analysts predict that the amount of data available will be fifty times what it is today;
- In 1990, it cost $527 for one million transistors. By 2012, that cost was reduced to $0.05;
- In 1992, storing information cost $569 per megabyte. In 2012, it was $0.02. (SIG 2016)

The modern information environment is also characterized by an exponential growth in the value of networked connections. This is best understood as the effect of communication technology, the Internet, and social networks. Identified as Metcalfe's Law, it states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2) (Kittredge 2011). The law is often presented pictorially using telephones, as in **Figure 1**, below. It takes two telephones to make just one connection; however, five telephones will make ten connections, and twelve make sixty-six connections. The power of this law is clear when considering the use and impact of social networks and technology on the information environment. As more people become part of the network, the value increases exponentially, meaning that its reach and ability to influence populations are hugely important.

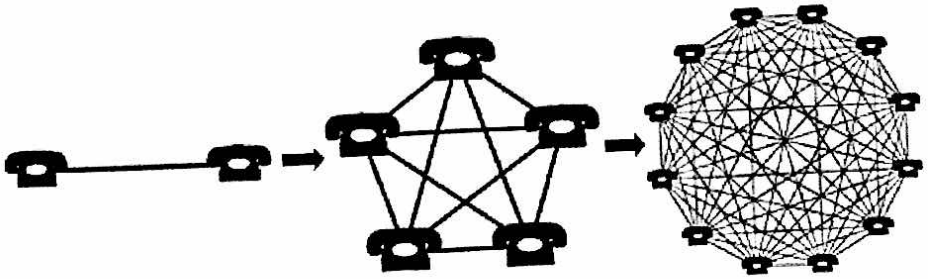


Figure 1: Metcalfe's law visualized

The information environment is not the sole province of nation states, or even large organizations. The relatively low cost of information technology, data storage, access to networks, and advanced software applications enables nearly anyone to participate, interact, and *affect* this domain. It is here that most forms of communication, social and economic interaction, and daily life occur.

Advanced technology has enabled human interaction with the physical environment on an immense scale. A single entrepreneur, such as Jeff Bezos, founder of Amazon, can amass enough resources to conduct an underwater expedition to recover the F-1 Thruster Engine from the

Apollo 11 Rocket off the ocean seabed (Bezos 2015), while a scientific research organization such as the Woods Hole Oceanographic Institute can sport an entire fleet of autonomous underwater vehicles (WHO Institution 2015). Elon Musk can found a commercial space exploration company, known as SpaceX, and become the first company to launch a vehicle and berth it with the International Space Station in 2012 (Harwood 2012). Of course, history is not unfamiliar with great technological and engineering feats or inventions. However, the *scale* with which humans are able to interact and influence one another has profoundly changed. By 2012, more than one third of the world's population had Internet access; 6.4 billion had a cell phone subscription; and Facebook had reached one billion subscribers (Techblog 2013).

Just as important, new analytic technologies and methods permit large volumes of data to be collected, evaluated, analyzed, and used to gain insight and make decisions. What was once the province of governments and large corporations, these 'Big Data' capabilities are available everywhere and to everyone at minimal or no cost. Almost all forms of social function and interaction can be captured, analyzed, synthesized, and perhaps even predicted at growing confidence levels. War being an intimate form of social interaction, the application of Big Data on military operations and national security could be profound. In the information domain, *anyone anywhere* can participate in war and conflict. One need only consider the implications of the Internet hacker group 'Anonymous', which has conducted operations against nation states such as North Korea in response to its attack on Sony (Bazzle 2014), as well as operations against ISIS (Griffin 2015). Combat operations in the information domain can be expected to involve multiple participants, greatly complicating military decisions.

However, it would be a mistake to overemphasize the importance of technology, to include hardware and software. Technology is merely the tool, the means, to acquire information. And information is the critical resource in the Phase 0 conflict. The ability to detect, deter, and (if necessary) defeat adversaries will be dependent on information. To date, America's adversaries appear to be taking a holistic view of and approach to how information is harvested and employed in conflict, as well as how it might be denied to the United States. In the cyberspace domain, Russia, China, and others conduct operations and influence media in order to shape a new environment and change the *status quo* without having to resort to kinetic conflict.

Does Phase 0 Work Anymore?

Traditionally, the United States sees itself as either at peace or at war. This bifurcated approach colors the legal, diplomatic, political, economic, and military lenses through which it engages actors in the world. During peacetime, the U.S. conducts steady state operations, which imply maintenance of the *status quo* (certainly not conflict). Relationships are largely static, and states are not contesting one another in the military domain. This is a legacy construct from the great wars in Europe and the Pacific in the 20th Century. The elements of this understanding include

- an emphasis on preventing wars rather than shaping environments;
- a view of risk centered around losing wars rather than the possibility of losing the peace; and
- a desire to excel at high-end warfare over confrontations which may fall short of violence.

Peacetime military planning and operations reflect this view. The U.S. military's handbook on operational planning, Joint Publication 5.0, defines Shape (Phase 0) as "Joint and multinational operations—inclusive of normal and routine military activities—and various interagency activities ... performed to dissuade or deter potential adversaries and to assure or solidify relationships with friends and allies". Shaping requirements tend to occur "in the context of day-today security cooperation" (Joint Chiefs of Staff 2011). Only when adversaries begin to conduct undesirable actions would the military shift to Phase 1 (Deter), which would include demonstrating capabilities and mobilizing joint forces. Failing deterrence, the military will act to "seize the initiative" (Phase 2), and "dominate" the adversary (Phase 3). Once defeated, the military will conduct stability operations (Phase 4) in order to enable local civilian governance (Phase 5), returning to peacetime shaping operations (Phase 0). The key discriminators between these phases and the American understanding of peace and war are the presence of kinetic violence and the level of military effort. 'Shaping' only occurs before and after conflict. See **Figure 2** below.

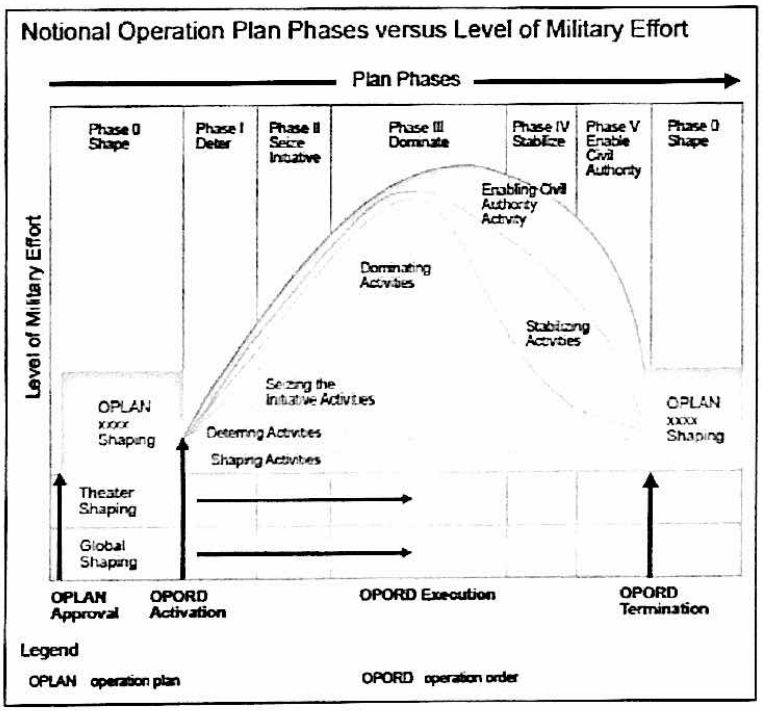


Figure 2: Notional operational plan phases versus level of military effort (Joint Chiefs of Staff 2011)

The American military has enjoyed considerable success, especially recently, at employing its kinetic capabilities. Perhaps it is because of this that adversaries, other than terrorist organizations, have gone to great lengths to come right up to the line of direct military violence, without crossing it. This is especially true in the cyberspace domain, where much of the information war is fought. North Korea, Iran, Russia, and China have all used cyberspace during 'peacetime' as a platform from which to violate national borders and sovereignty by emplacing tools (specifically, cyber weapons) on our critical infrastructure, stealing intellectual property, and attacking U.S. industry as well as government and military networks. They are developing strategies and concepts designed to deny and disrupt U.S. information networks in order to achieve strategic objectives. They understand American political, cultural, and legal reticence to

act during peacetime because *we do not recognize this category of conflict as being 'war'*. When the U.S. does finally act, it is often too late or insufficient to influence or deter nimbler authoritarian regimes such as those mentioned above. Russia and China provide two examples and are worthy of a closer look.

Russia's Hybrid War Strategy

The term 'hybrid war' suggests the combined use of previously understood concepts related to war, to include conventional, irregular, political, information, or otherwise. Therefore, Russian hybrid war may not represent a new way of fighting, but rather a recognition that modern war still relies on "the integrated utilization of military force and forces and resources of a nonmilitary character", and, "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force" (The Military Doctrine of the Russian Federation 2010).

Regardless, Russia has been able to achieve military objectives on its periphery through a socially savvy, subtle, and ambiguous form of war, the main elements of which are *information confrontation*, *destabilizing operations*, and the use of *conventional forces*.

Information confrontation, which harkens back to Soviet doctrine on 'Active Measures" (Boghardt 2006), uses disinformation, misinformation, and planted information delivered via the Internet, social media, and traditional media. It draws particularly on Soviet-like themes of anti-Nazism, the threats to Russian civilization, Western "information aggressions", and "destabilization strategies" against Russia. It has developed a significant "[I]nternet troll" army—a new, secretive, state-sponsored agency designed to spread propaganda, attack critics, and sow domestic discord in targeted countries (Chen 2015).

Confrontation in the information environment is followed up by clandestine political *destabilizing operations* against the political apparatus of the target country. It might seize certain state or public media, attack certain facilities or smear them as agents of oppression, or fund and supply separatist insurgents. Examples would be operations which falsely showed ethnic Russian minorities being persecuted in the Ukraine (2014), Georgia (2008), and Estonia (2007).

To support these efforts, Russian *conventional forces* would be mobilized and deployed to the border region of the target country to serve as a form of intimidation, to supply Russian-supported separatists, and—if necessary—to conduct incursions or to intervene directly.

The use of cyberspace operations to support hybrid warfare strategy has three components: the targeting of the domestic population of a country using diplomats, hired 'experts' and academics to influence perceptions and opinions; the use of information operations to control the message; and offensive cyber operations against computers and communication systems. Information is used to *confuse*, *paralyze*, and *subvert*, unlike the American/Western model, which uses information to *persuade*.

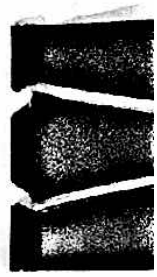
Chinese Informationized War

China's cyberspace operations and strategy are driven primarily by preservation of Communist Party (CCP) rule. Domestic security, economic growth and modernization, territorial integrity, and the potential use of cyberspace for military operations center on maintaining the CCP's power. Even its diplomatic and international policies are built around giving China maneuvering room to interpret international norms, rules, and standards to serve domestic needs, principally through the primacy of state sovereignty. China must balance economic growth and globalization with maintaining the Party's firm grip on power, which creates tension. Not only is Internet usage controlled and censored, but it is also a tool for state propaganda (MacKinnon 2008).

Cyberspace operations are central to the People's Liberation Army (PLA) concepts of "informationized warfare". As Watts (2014) has written, the PLA sees war transitioning to an "informationized" state "in which informationized operations are the main operational form and information is the leading factor in gaining victory". Information is a resource to be harvested and exploited, as well as denied to the enemy or manipulated for advantage. Nations and militaries "can be wealthy or poor in this resource. Overall wealth in information is what will ultimately matter most in peacetime competitions, crises or military conflicts" (Watts 2014).

Timothy Thomas (2014) has identified several components to Chinese military thinking, to include

- a more broad and analytic framework that holistically incorporates information-age strategy;
- while remaining prominently Marxist, it "examines the strategic environment through the lens of objective reality and applies subjective judgment to manipulate that environment to one's advantage";
- the use of stratagems integrated with technological innovation, creating a hybrid combination targeting the adversary's decision-making process to induce the enemy to make decisions China wants;
- the constant search for *shi*, or strategic advantage. *Shi* is thought to be everywhere, "whether it be with the use of forces, electrons, or some other aspect of the strategic environment"; and
- the object of "deceptively making someone do something ostensibly for himself, when he is actually doing it for you".



According to Jullien (1999) *shi* is the "concept born of disposition ... of a process that can evolve to our advantage if we make opportune use of its propensity". Chinese military thought seems to differ from the Clausewitzien understanding of confrontation, becoming focused on *shi* rather than "ends" and "means". *Shi* aims to use "every possible means to influence the potential inherent in the forces at play" to its own advantage, before any engagement or battle takes place (Jullien 1999). Therefore, the engagement never actually constitutes the decisive battle that Clausewitz envisions, because it has already been won. Chinese cyberspace operations support this strategy by

- gaining information through reconnaissance of cyber systems, and manipulating or influencing Western or American perception and technology to establish strategic advantage;
- using that reconnaissance information to position its forces, to locate vulnerabilities, and to be in a position to conduct system sabotage;
- in a crisis, using system sabotage to either render information technology systems impotent, or expose strategic cyber geography to establish offensive cyber deterrence (Thomas 2013).

Both Russia and China have shown considerable sophistication in their application of information war and cyber power to achieve their strategic objectives. They have taken advantage of America's bifurcated understanding of 'peace' and 'war' by always remaining just left of the line of direct kinetic conflict, seeking to change the facts on the ground and to obtain better position. Originally, Western leaders had hoped that the spread of information technology and the Internet would undermine authoritarian leaders worldwide, ushering in social and democratic change. Instead, it has become a tool for espionage and industrial theft, a domain of military confrontation and a political weapon.

From Shape to Competition

Recognizing that the U.S. is engaged in a long-term competition with nation-state adversaries who will likely not use overt force suggests that the current phasing construct may be inadequate for modern competition between great powers. War remains no less violent, dangerous, and fraught with catastrophic potential. But the current competition has its own danger, not the least of which is that the United States might find itself on the losing end of a long-term competition without a shot being fired. Worse still, the U.S. might embark on a devastating war that it could not hope to win because it allowed the adversary to achieve an overwhelmingly advantageous position.

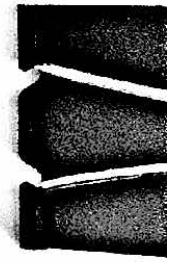
Conflict in Phase 0 centers around 'position', which Jacqueline Deal (2014) describes as a "disposition of power so favorable that the use of military force is unnecessary to secure your interests". The game of chess provides an instructive example of 'position'. Andrew Marshall recently noted that "most of the game is not directly aimed at checkmating the opponent's king. Instead, the early and middle parts of the contest are about building a more advantageous position from which checkmating the opponent almost plays itself out" (Watts 2014). Indeed this is why most competitive games of chess end not in checkmate, but rather in concession or a draw. The player on the losing end knows that he or she will lose, perhaps in a finite number of moves. That is the essence of having the most advantageous *position* and winning without fighting.

There are a number of steps that might be taken to better posture American power in this era of persistent conflict at the level of grand strategy and specific to the Department of Defense. First, the U.S. must better conceptualize its understanding of the impact of information on operations *without* mirror imaging its adversaries. Competitors such as Russia, China, and others view information through their own cultural lens and history, and it would be a mistake to merely mimic them. Instead, it is better to consider ways to leverage America's natural strengths in the information environment. Recent studies on global attitudes toward democratic principles such

as freedom of expression, religious freedom, gender equality, and free elections show widespread support. Majorities in 32 of the 38 countries surveyed by the Pew Research Center in 2015 indicated that it is important to live in a country where people can use the Internet free of government censorship (Pew Center 2015a). Overall, global surveys suggest the U.S. is viewed more favorably than China (Pew Center 2013), Russia (Pew Center 2015c), and Iran (Pew Center 2015b). These attitudes toward America can provide unique operational advantages in the information space. Given its adversaries' doctrines and concepts of information war, the U.S. can also expect them to attempt to undercut these advantages through deception and disinformation campaigns.

Secondly, the U.S. should take greater advantage of the alliance network it currently enjoys. In major areas of trade, security, and diplomacy, the U.S. has developed deep relations with like-minded nations, as well as with nations that share critical interests. This is an advantage not enjoyed by America's principle adversaries. While the U.S. and allies have done much to improve security cooperation and interoperability between military forces, a coordinated information competition strategy will likely require deeper collaboration on strategic communications, intelligence collection and sharing, and operations in cyberspace and the electromagnetic spectrum.

Next, new legal and policy frameworks will be necessary to compete. U.S. law and policy must be explicit regarding the use of cyberspace as a means to steal industrial technology and to conduct preparatory operations on critical U.S. infrastructure, as well as its adversaries' use of America's Internet backbone to conduct information operations campaigns. These frameworks must provide decision makers with sufficient authorities and latitude to conduct high tempo operations with the agility to maneuver quickly to conduct offensive and defensive fires. These authorities have to extend to civilian law enforcement, intelligence and counter-intelligence agencies, and the National Guard, as well as to the military.



In addition, the U.S. must acknowledge the importance to law and policy that the economic arrangements between the U.S. government and the technology industry have. The recent revelations by Edward Snowden that key technology companies cooperate with the U.S. government have placed significant pressure on those companies to distance themselves. On top of that, the very public debate between Apple and the Department of Justice on encryption, privacy, and counter-terrorism has become a hotly charged political topic. Serious issues of trust and transparency complicate the relationship between the U.S. government and industry—issues which likely do not affect China or Russia. Yet this economic relationship is critical to America's ability to compete. The government—and especially Department of Defense and law enforcement—should take steps to develop new partnership mechanisms which promote information sharing and professional networking at the lowest level with industry, as well as enable timely action. Major telecommunication firms, which serve as the backbone of the Internet, require timely, actionable information in order to coordinate responses to malicious activity. The government and military must engage with the technology industry *in the way they engage with one another*—via personal trust and actionable information. Policy and law should permit the private sector to act in response to attack or theft of intellectual property and should devise sanctions to support American industry and impose costs. The U.S. must also take a holistic view of technology sharing, sales, and the use of foreign firms to provide information

services at home. The use of foreign technology and foreign vendors by the U.S. government should be carefully scrutinized, coming on the heels of the recent theft of personal information of millions of federal government employees, which was likely the result of the Office of Personnel Management's (OPM) hiring of foreign contractors to manage personnel records (Bertrand 2015). Adversary governments look at their indigenous information technology companies as strategic resources, and the U.S. needs to approach them in the same way. The U.S. would be challenged in doing so because many large American technology firms (for instance, Apple, Microsoft, and Intel) are global corporations, and global markets drive their behavior. However, as previously mentioned, global attitudes largely reflect American core values, and the U.S. will have to balance competing interests.

Also, new operational concepts will be needed, and these concepts have to favor active response over defense. Adversaries must be made to suffer costs, and the U.S. should not feel obligated to respond in kind. This is not to say that network defense is not still required; it is. But network hardening must be coupled with capabilities that permit rapid reconstituting of networks and the resiliency to fight through network attacks. This network hardening should also include the development of alternative command, control, and communication networks that can be fielded quickly in the event of a crisis. For example, microsatellites and nanosatellites can be deployed to either rebuild disrupted networks or add redundancy to existing networks, reducing adversary confidence that it can effectively deny information to the United States during a conflict.

Importantly, responses need not be in kind or symmetric. In response to continued theft of intellectual property by China, the U.S. might inform the technology industry that the government is unable to protect proprietary information; therefore, doing business in China might not be worth the cost. The U.S. might also sanction firms that use stolen intellectual property, as well as third-party firms that do business with them. Another option would be to provide private firms latitude in their own ability to respond to attacks on their own networks or attempts to retrieve stolen intellectual property. In response to governments which implant cyber weapons on American public infrastructure, such as power companies, telecommunication nodes, or the financial industry, the U.S. might respond by developing and demonstrating its own capabilities in a series of public exercises and wargames, adopting a posture of 'mutually assured disruption'—*even during 'peacetime'*.

In addition, new operational concepts in Phase 0 should also include more integrated cyber surveillance, reconnaissance, and preparation of the cyber environment. These military operations should emphasize delivering military effects on networks of interest versus the collection of foreign intelligence, which is the role of the intelligence community. Because detection and attribution are problematic in cyberspace, military cyber forces are well postured to conduct enhanced information operations, denial and deception, and operational security activities. Also, military cyber forces can conduct cyber activities designed to enable strategic communication or shape and influence the dominant narrative as part of a larger 'whole of government' or 'whole of nation' effort.

Next, new concepts must also approach information holistically and provide commanders with social, political, economic, diplomatic, technical, friendly, and enemy information. The U.S. approach to information operations has tended to remain stove-piped into a series of disparate

and uncoordinated communities such as 'signals intelligence', 'electronic intelligence', 'electronic warfare', 'cyberspace operations', and 'C4ISR'. This fragmentation only exacerbates the difficulty in developing a comprehensive, holistic approach to information warfare and integrating information operations into larger military operations. Modern war takes place in an information domain in which the combatants are operating side by side with non-combatants. It is a form of urban war taken to an extreme. Commanders will need to have visibility on a whole host of classified and unclassified information in order to develop strategies, conduct operations, and anticipate reaction to friendly and enemy actions. U.S. planners have attempted to address this need with the development of the Joint Information Environment (JIE); but even here, critical vulnerabilities remain, especially to the physical transmission layer (Dahm 2015).

Military planning emphasis must, therefore, shift from Phase III 'Dominate' targets—those typically attacked during major combat operations—to Phase 0, with a corresponding level of effort. Intelligence collection necessary for planning must also shift to a system-to-system analysis of the information networks and information capabilities of adversaries on a much deeper and finer scale. The adversaries' centers of gravity (COG) will likely change from traditional military targets to regime information control systems and networks, communication networks, economic and industrial infrastructure, trade nodes, C4ISR, and other nonmilitary or dual-use systems. Many of these networks of interest are closed or difficult to reach from traditional IP space and, therefore, may require off-net operations to gain access. These off-net access operations, whether enabled via the radio-frequency spectrum or human-enabled, require considerable lead time, intelligence preparation, and resources. A recent RAND study looked at various tools the U.S. could use, short of direct kinetic military action, in order to compel and deter competitors, including some (financial sanctions, cyberspace operations) mentioned here (Gompert & Binnendijik 2016). The key is that non-kinetic coercive power is increasing in both importance and effectiveness, and military planning and effort should reflect this shift.

Conclusion

The American perspective on war and peace must adapt to an era of persistent conflict, ambiguous results, and a different theory of victory. Department of Defense planning using a phasing construct that emphasizes Phase III military operations over Phase 0 is likely hindering our conceptual understanding of conflict today. Phase 0 is best understood as 'persistent conflict' rather than 'steady state', and the U.S. must learn to act in this Phase, cultivating an advantageous position relative to its adversaries. Information is the critical resource in Phase 0, made much more important to modern conflict due to the growth in processing power and the power of social networks. The U.S. must develop a holistic, comprehensive understanding of the impact of information on operations if it is to compete successfully and win in Phase 0.

References

Bazzle, S 2014, *ANONYMOUS announces vengeance on North Korea for Sony hack with #OPRIPNK*, viewed 9 April 2016, <http://www.inquisitr.com/1691688/anonymous-announces-vengeance-on-north-korea-for-sony-hack-with-opripnk/>.

Bertrand, N 2015, 'The U.S. agency plundered by Chinese Hackers made one of the dumbest security moves possible'. *Business Insider*, 18 June.