Preface

Over the years, technological advances have often had a substantial impact on warfare. Just in the past century, the development of machine guns, heavy artillery, armored vehicles, airplanes, and nuclear weapons have each dramatically disrupted established tactics and forced militaries to analyze the nature of these new technologies. However, the mere arrival of a new technology does not ensure that an organization will utilize it successfully. Early versions of new weapons typically fail to equal the full range of capabilities of the mature technologies they intend to replace, and often many competing technological development paths offer a multitude of potential futures. Consequently, the decisions made prior to the outbreak of conflict often prove crucial to which militaries prosper from technological advancements and which fail to utilize these new abilities to their full potential. After all, both the British Royal Navy and the United States Navy developed aircraft carriers following the First World War, but, of the two, only the Americans developed the technology into a war winning set of capabilities and doctrine. Similarly, every major European power built tanks in the interwar period, but only the Germans developed blitzkrieg.

Today, the dawn of cyberwarfare has forced militaries around the globe to reassess their standard operating procedures and consider how the conflicts of the future will change as a result of these developments. Every military has a handful of visionaries and theorists who will determine their nation’s concept of cyberwarfare and establish expectations for how it will impact the wars of the future. Among the most important aspects of this vision will be how they believe cyber will impact the balance between the offense and the defense. When strategists expect that the offense holds the advantage and that wars will be quick and painless, it can lead to crisis, instability and more conflicts. In contrast, when they believe that the defenders hold the advantage, it reduces the outbreak of conflict and buys time for diplomacy to find alternative
solutions. Consequently, understanding how the major world powers view the cyber domain’s impact on the balance of power contains urgent lessons for the future of international relations.

In order to investigate this phenomenon, I will first briefly explain the precepts of the Offense-Defense theory. Then, I will clarify what types of cyber actions do and do not qualify as cyberwarfare. Next, I will explore how the underlying tenets of Chinese and American cyber doctrine correlate with the major predictions of the theory. Finally, I will enumerate a series of policy proposals to strengthen American cyber strategy and enhance its ability to win the cyber competition against its enemies.

**Offense-Defense Theory**

The offense-defense balance has become one of the most widely used theoretical constructs in international relations. It posits that technical and geographic factors affect whether the offense or defense has the advantage in any potential war, and that this will influence how two potential combatants prepare for conflict and react to a crisis. Many casual observers misunderstand the theory and consequently misinterpret whether a particular technology favors the offense or not. For example, nearly everyone would agree that a bulletproof vest is a defensive technology. However, many would incorrectly assert that firearms provide an advantage to the offensive. Although a firearm can kill or injure people, the fact that a weapon inflicts damage does not necessarily mean that it favors the offense. In fact, when two armies face each other on the battlefield, the defensive force can fire their weapons while aiming from behind cover. In contrast, the attacking force must often cross open terrain even as their movements leave them unable to return fire accurately. This causes firearms to favor the defenders, on balance. Similarly, a nuclear weapon mounted on an ICBM will only rarely prove a useful weapon to use on the tactical defensive, since friendly forces will suffer nearly as much harm as enemy forces. However, deterrence and Mutually Assured Destruction, which rely on nuclear weapons, have in fact shifted the balance in favor of the defender, since an attacker cannot profitably attack a nuclear state. Therefore, any determination of whether cyber favors the offense or the defense cannot simply examine whether it is easier to hack a particular computer or whether it is easier to prevent someone from hacking that computer. Instead, even if hackers hold the upper hand over system administrators, any evaluation of the offense-defense balance must consider whether or not the resulting cyber weapons would prove more useful in assisting attacking military forces or whether they would prove more helpful to defending forces wishing to thwart an attack.

---

2 Ibid
Some theorists have criticized the Offense-Defense theory on the grounds that, much like Heisenberg’s Uncertainty Principle, one cannot actually perform the necessary calculations to determine the exact offense-defense balance at any given time. In fact, one does not need to ascertain precisely whether or not a technology actually favors the offense or the defense. Instead, in order to comprehend pre-conflict behavior, one merely needs to know which side policymakers believe holds the upper hand. History is littered with examples when strategists incorrectly assessed the prevailing balance; France most notably falsely believed the balance favored the offense in the First World War, only to then incorrectly conclude that the defense held the advantage in the Second. Even though French military and political leaders had incorrectly assessed the offense-defense balance, they took action based on their beliefs. Consequently, if one can determine how influential strategists perceive the offense-defense balance, this will provide substantial insight into which policy choices a nation’s leadership will make prior to the onset of hostilities. In these historical cases, military theorists and policymakers made statements that allow a researcher to clearly determine their beliefs; the same holds true for the cyber domain today.

The offense-defense balance theory makes several predictions as to how states will behave when they believe the balance favors one side or the other. We will consider predictions in the case where the adversaries cannot distinguish whether or not their opponent has adopted an offensive or defensive posture, since experts widely agree that the cyber realm maintains this characteristic.

In such a world, when the offense is perceived to hold the advantage, it generates enormous pressure for nations to engage in arms races and to launch preemptive attacks during a crisis period. Revisionist powers feel these strains most acutely, since they desire to alter the world to achieve their goals in any case. However, even status quo powers may find themselves compelled to initiate hostilities out of fear that their enemy may reap the tactical benefits of doing so if they hesitate at the moment of decision. In contrast, a world where the defense maintains the upper hand displays more stability. Although a revisionist power can acquire enough arms to initiate a war, its adversaries typically can detect these actions far enough in advance to negotiate an acceptable compromise or commence their own military buildup. Therefore, correctly determining how different powers perceive the offense-defense balance should allow an expert to make predictions as to how they will behave.

---


Defining the Cyber Battlefield

Before determining how policymakers perceive the offense-defense balance in the cyber domain, it is important to clarify what kinds of cyber operations affect this balance. Every day, hackers scan and probe American networks, including military networks, looking for a vulnerability they can exploit. However, despite the rhetoric of many government officials and cyber experts, the copying or deleting of files by malicious actors typically does not rise to the level of cyber warfare. One widely used taxonomy establishes four categories which most cyber operations fall into: economic espionage, political and military espionage, cyber crime, and cyber war.\(^5\) Others sometimes add categories such as cyber propaganda or cyber terrorism to this list. These definitions differentiate cyber warfare from other types of cyber operations by the intended destructive and political effect of the programs employed, noting that cyber war must “attempt to damage or destroy US military capabilities (including our informational advantage), critical infrastructure, or other civilian targets.”\(^6\) General Keith Alexander, former head of the National Security Agency and Cyber Command, agrees, defining cyber warfare as “using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability, while protecting our own.”\(^7\) By these definitions, China’s stealing of American corporate secrets or its hack into the Office of Personnel Management do not qualify as cyber warfare. Even major incidents such as the Russian-Estonian conflict of 2007 do not qualify as cyber warfare, since none of the cyber weapons used had any meaningful impact on the combat potential of the two combatants.

Defining cyberwarfare in this way also limits the number of potential actors who could wage a serious conflict utilizing cyberspace. Writing an intricate software program akin to the Stuxnet worm requires many man-years worth of software engineering effort. Consequently, individual hackers and even most nation-states would not possess the capabilities needed to create weapons of this type and complexity. Some private sector actors, such as Microsoft, Amazon, or Google, do retain the necessary software talent and financial resources to design and deliver a malicious program of that magnitude, but doing so would be well outside their institutional identities and self-interest. While private sector entities might retaliate against acts of economic espionage, they would likely refrain from engaging in a true cyber war independently from their host nation-state.

Chinese theory and doctrine

To understand China’s view of cyber conflict, one must first understand its position in the international system as a whole and the overall vision guiding its armed forces. China envisions

---

\(^6\) Ibid
itself as a rising power emerging from a period of unusual weakness. Prior to the reforms 
instituted by Deng Xiaoping, China had relied on Mao’s doctrine of “People’s War” for its 
defense. This derived from Mao’s experience as a leader of guerilla forces fighting against the 
Japanese and Chiang Kai-shek’s Kuomintang government. Even after independence, the Chinese 
did not expect that their air and naval forces possessed the strength needed to prevent enemy 
forces from invading and attacking their homeland. Instead, the Chinese people would gradually 
wear down and exhaust their attackers, prevailing in a long war of attrition. However, China’s 
economic recovery has presented its communist government with new options. China has 
substantially increased military spending across the board and its military modernization efforts 
have both shrank and modernized its forces. China’s increased aggressiveness towards its 
neighbors reflects the degree to which these new capabilities have presented its leadership with 
ew policy options. The People’s Republic of China (PRC) has reinvigorated an old dispute with 
Japan over ownership of the Senkaku (or Diaoyu) Islands as well as sparring with the Vietnamese 
and Philippines governments over territorial disputes in the South China Sea. This context clearly 
places China in the role of a revisionist state in the international system, since China wants to 
alter the status-quo to reflect its improved standing in the world.

Changes in the nature of warfare

China’s leadership recognizes that their external ambitions will most likely bring them into 
conflict with the United States. Many of their territorial disputes involve American allies whose 
security arrangements with the United States assure them of receiving American assistance 
during any crisis with a foreign power. In response, Chinese officials have devised a new strategy 
to guide their preparation for any such conflict. This strategy, laid out most completely in The 
Science of Military Strategy, calls for China to prepare to win a “local war under high-tech 
conditions.” As the book explains, China believes that nature of modern warfare has 
fundamentally changed and that this reality will eventually result in meaningful alterations to the 
international system. First, its scholars believe that “The size and influence (of war) are limited. 
Even the war in which some big powers are involved is not likely to develop into high-intensity 
worldwide war because of the asymmetric contest. … The elements to restrain war have been 
strengthened, and war is moving in the direction of limited purposes and controllable size.”

Economic concerns exert similar influence over the size and duration of warfare. At the same 
time, information technology has “greatly improved operational effectiveness and efficiency, 
which has laid (the) material and technological basis for war to become controllable and small-

---

8 Guangqian, Peng and Yao Youzhi. The Science of Military Strategy (Beijing, China: Military Science Publishing 
House, 2005), 398.
Finally, the Chinese believe that warfare has become more cost-effective as the net result of these various trends. The *Science of Military Strategy* explains:

> The contradiction between the high strategic cost of war means and the political aim which serves the comprehensive national power competition becomes more prominent ... The new technologies revolution represented by information technology has brought about the rapid development of military technologies and the new breakthroughs of operational methods ... Israel’s bombing of the Iraqi nuclear reactor (1981), the US attack on Libya (1986), multinational forces’ hit-home strike ... in the Gulf War (1991), NATO’s air raids ... in the Kosovo War (1999) all prove that high-tech is serving as a more effective tool to achieve military aims. It is possible to avoid the high political and military cost which was once unavoidable in the traditional military occupation.\(^9\)

Each of these military examples resulted in victory for the side possessing superior information weapons with minimal need for a drawn out and expensive ground component to the campaign. Chinese strategists clearly intend to use these historical precedents as a model to minimize the costs of any future war they might need to wage.

Additionally, Chinese strategists believe that technological advancements and geopolitical realities have changed the fundamental nature of warfare. As a consequence, modern warfare has become smaller, quicker, and more effective. They explain that, “The features of the development (high-tech, local war) are as follows: The cycle of war development is shortened. The political objectives of war become limited. The size of war turns more controllable and smaller.”\(^11\) At the same time, within the limited timeframe and objectives of the conflict, the theater of operations can expand dramatically. As they explain, “It is a kind of war characterized by its comprehensiveness with limited objectives. The war space is endlessly expanded, and there is no clear dividing line between the front and the rear. Military and nonmilitary targets are integrated into one thing. All the corners and aspects of the enemy are within the range of strike.”\(^12\) The innate ability of cyberweapons to ignore traditional geographic limitations makes them particularly attractive to Chinese officers for these purposes.

Most importantly, Chinese theorists believe that “informationalization” acts as a key factor shaping the nature of modern warfare. As they explain, “The information security has become the most important security element. In this case, without information security, there would be no political safety, economic safety, military security, science and technology safety, culture security, etc. ... No weapon could cause such strategic damage.”\(^13\)

---

9 Ibid, 401.
10 Ibid, 402.
11 Ibid, 404.
12 Ibid, 406.
13 Ibid, 122.
encompasses some parts of the cyber domain beyond just Computer Network Attack and other acts of cyberwarfare, they do foresee that cyber will play a critical role in making core portions of their strategy actionable. As they write, “Cyberized weapons provide effective means for achieving war purposes rapidly. In information operations, a small-scale tactical operation can sometimes achieve strategic or operational purposes; therefore the operational limits of traditional strategic, operational, and tactical levels are increasingly blurred. The development of information technology also makes geographic distance lose its traditional significance. Any place that information can reach might become the battlefield of information warfare. The targets in the strategic depth are as vulnerable as targets in the theater.” As demonstrated above, the comprehensive nature of war plays a key role in Chinese doctrine, and cyber offers the possibility to overcome their weaknesses in traditional means of power projection, such as warships or aircraft.

**A new tempo of operations**

Just as importantly, cyber plays a critical role in quickening the tempo of war, which acts to reduce its total duration. As Chapter 20 explains, “In terms of time, war has become (an) all-time, high-tempo contest striving for minutes or even seconds. It is a war to employ brand-new informationalized operational means, for the information dominance becomes the decisive element for the victory.” Chinese doctrine even expects that many wars will shorten to the point that they may consist only of a single, intense battle. As its architects explain, “In the high-tech, local war, the gathering and release of war energy can achieve a fairly fast speed ... The combat efficiency doubles and redoubles, so that the war becomes more resolute and ends more quickly. The side that enjoys high-tech advantages often employs a large number of high-tech weapons and carry out all-round and all-in-depth intense attacks in order to defeat the enemy at one fatal strike. The war tempo is quickened and the war process is greatly shortened. It has become a guiding rule for war launchers to accomplish the whole task at one stroke. ... The first battle may be the last one, for its victory may put an end to the whole war.” Recent military operations such as the First Gulf War, the Israeli conflict with Syria in 1982, or the US intervention in Libya, have reinforced the Chinese understanding of the tempo and impact of informationalized operations.

Given the fast pace of modern warfare, where the critical opening salvo may determine the course of the conflict, Chinese doctrine emphasizes the need to seize and maintain the initiative through offensive action, preferably with a preemptive strike. Chapter 16 includes a section entitled “Information Operation is directly linked to the gain and loss of war initiative. Strategic

---

14 Ibid, 339.
15 Ibid, 406.
16 Ibid, 417.
Information Operations should establish the thought of giving priority to attack and combining attack with defense.” It elaborates on this theme by explaining that in any military conflict China must first launch “preemptive attacks to gain the battlefield initiative. Launching information attacks actively is the key of seizing information superiority and battlefield initiative. ... Defensive operations can neither directly threaten the enemy’s information systems nor greatly weaken his information superiority. Only information attacks can directly disturb and destroy the enemy’s information systems ... So only by combining offense with defense and giving priority to offense, can one seize information superiority totally.”

Given the relative weakness of China’s conventional forces compared with their high-tech opponents and their limitations in areas such as logistics, decentralizing authority to junior officers, and adapting to unknown situations, the first combat operations will most likely hold even greater importance for the People’s Liberation Army than it typically would for their opponents.

Is Chinese strategy defensive?

Some documents describing China’s strategic plans attempt to characterize China’s strategy as defensive. However, the Chinese do not necessarily see a defensive strategy as contradicting the need to launch a preemptive war to gain the initiative. As Chapter 24 explains, “We should do all we can to dominate the enemy by striking first. Once the enemy invades our territory and offends our national interests, it means that they enemy has already fired the first shot strategically and crossed the border of our strategic defense. Thus, we get the freedom to conduct self-defense operations ... we should not passively fight against the enemy in our border regions ... On the contrary, after the launching of the war, we should try our best to fight against the enemy as far away as possible.”

The war against India in 1962 provides a good example of this from the Chinese perspective – even though China fired the first shot “tactically”, India had fired the first shot “strategically” and consequently China’s commencing combat operations with a surprise attack qualified as a defensive military action. Similarly, China may regard operations against opponents in disputed territories as “defensive” even if the Chinese military opens hostilities.

Additionally, some Americans have described China’s overarching strategy as one of Anti-Access/Area Denial (A2/AD). When phrased this way, it would seem to imply that China’s leaders primarily intend to utilize a defensive strategy by merely deterring American forces from approaching and attacking their homeland (or destroying them if they attempt to do so anyway). However, while China’s armed forces could employ many of these technologies on the tactical defensive, China’s strategy is best understood as ‘local’ as opposed to ‘defensive’. Many of the

17 Ibid, 345.
18 Ibid, 461.
19 Ibid, 426, 459.
relevant A2/AD Chinese weapon systems have ranges that limit their utility to the East Asian theater. To an observer located outside the region, these weapons might appear to have a primarily defensive purpose. However, a citizen of a nation such as Taiwan or Japan whose homeland lies within range of these systems views them very differently. These allies fear that a Chinese military strong enough to deter intervention from the United States could utilize this freedom to engage in acts of aggression against its neighbors, secure in the confidence that the United States could not successfully launch a counterattack to reverse its gains. In fact, this dynamic reflects a modern instance of the well understood Security Dilemma whereby acts that improve the security situation for one power, even if primarily defensive in intent or even in nature, can threaten neighboring states and require counterbalancing actions.

**Confirmation through actions**

Recently, China’s actions have mirrored its words. In its most recent military reorganization announced on the last day of 2015, Xi Jinping ordered the creation of a new military service called the Strategic Support Force (SSF). Chinese official media published an interview with Yin Zhuo, a rear admiral in the PLAN specializing in cyber issues, explaining the purpose of the force. As it states, “the major mission of the PLA Strategic Support Force is to give support to the combat operations so that the PLA can gain regional advantages in the astronomic war, space war, network war, and electromagnetic space war and ensure smooth operations. ... ‘All these are the new fields that determine whether the PLA can win in the future battlefield.’” Although the recent announcement of this reorganization makes it difficult to publicly confirm exactly which units will move under this new organization, experts believe the Strategic Support Force will ultimately encompass Chinese military units as diverse as its Electronic Warfare personnel, Intelligence/Surveillance/Reconnaissance assets such as the Aerospace Reconnaissance Bureau and the tactical reconnaissance assets of the Second Department’s Second Bureau, as well as its signals intelligence and cyber forces. All in all, the creation of a new, independent service equal in stature to China’s army, navy, air force, and strategic rocket forces and unifying nearly every unit specializing in any form of information operations confirms China’s commitment to information warfare as an essential part of winning the high-tech local wars it believes represents the future of warfare.

---


Offense-Defense theory applied to Chinese practice

In light of the evidence presented above, the hypothesis about the offense-defense balance takes on a new relevance to contemporary affairs. It argues that three critical questions define how the offense-defense balance will affect international relations. First, how does the innovation in question affect the financial balance in war? In other words, for each dollar one state spends on buying weapons to support an attack, how many must its potential victim spend preparing itself to repel the assault?\(^{23}\) If the Chinese government has conducted a thorough, quantitative assessment of the net financial impact of cyber weapons on warfare, it is unlikely that any such information will make its way into the public domain where an American researcher could access it within the foreseeable future. However, the analysis made by China’s premier cyber warfare theorists indicates that at the very least they believe that modern advancements in information technology have shifted this ratio in favor of the offense relative to its previous position. They repeatedly refer to the ways in which information warfare has made waging hostilities more efficient. In particular, their belief that high-tech advancements can make expensive occupations of territory unnecessary provides direct evidence that they believe that war has become more profitable for an attacking state as a direct result of the key developments their doctrine focuses on. As the historical examples underpinning the offense-defense theory have demonstrated, under these conditions states become more likely to adopt revisionist attitudes and revisionist states are more likely to initiate conflict, drawn in by the apparent net profits that a low cost victory would obtain for them.\(^{24}\) China’s strategic thinkers appear to agree with these assessments.

The second major question asks whether a state should adopt an offensive or defensive posture under the current tactical conditions.\(^{25}\) If a state believes that attacking would provide the greatest chance of military victory, it will most probably react to an escalating crisis by launching an attack as soon as it fears its opponent might do so, regardless of whether or not initiating such an aggressive action would otherwise advance its interests. Beliefs in offense dominance become self-reinforcing, since an aggressor state expects its attack will inflict disproportionate damage on its enemy which in turn places the aggressor in an even more favorable position to launch future attacks. Consequently, the only rational response by any military to this situation is to launch an attack as quickly as possible during any major crisis which might escalate to war. Any other course of action would place the state in potentially mortal danger at the hands of an adversary prepared to reap the benefits of striking first. In contrast, when the defense holds the advantage, a state can adopt a defensive posture in relative safety, knowing that it can quickly


\(^{24}\) Ibid, 189

\(^{25}\) Ibid, 188
and cheaply outmatch its foes’ military power if they begin to display hostile intent. This characteristic leads to stability, since states have ample time to react to their adversary’s moves and the balance of power cannot be suddenly or unexpectedly upset. In China’s case, its doctrine clearly emphasizes the need to preemptively attack its enemies in order to seize and maintain the initiative. Its policies explicitly identify the requirement to strike first even in a conflict where China finds itself on the strategic defensive because of the nature of modern warfare. Such actions could hardly be better tailored to reflect the offense-defense theory’s predictions in the case where planners perceive that the offense holds the advantage and intelligence organizations cannot confidently distinguish between offensive and defensive force postures.

The final question asks how states in the international system perceive the speed of military operations. Under offense-advantage conditions, states will expect a quick tempo of conflict compared with defense-advantage conditions. As a direct consequence of this, states will tend to engage in destabilizing actions such as rapid arms build-ups. A threatened state cannot afford to ignore any increase in strength by a potential foe because the swift pace of conflict means that any imbalance in power, even a fleeting one, could place it in mortal jeopardy. As has been demonstrated above, China’s belief that the unique characteristics of modern wars make them shorter and more precise echoes these predictions. Its promotion of the Strategic Support Force to the status of an independent service will most likely also bring a fresh infusion of funding in the years to come. If this proves accurate and if China’s adversaries find themselves compelled to follow suit, it would provide a vivid demonstration of the prediction that these conditions should prove particularly fertile for the development and acceleration of arms races.

**American policy and doctrine**

In contrast to China, America occupies a very different position in the international system. The United States has sustained itself as the world’s hegemon since the end of the Cold War. Its alliances encompass most of the world’s second tier powers and it has little interest in conquering new territories or revising the current distribution of power given its leading position in hard power, soft power, and economic power. As such, it acts as a classic status-quo state within the international system. Typically, status-quo states prefer defense-advantage systems. Under these conditions, they can cheaply and effectively defend themselves against aggressors who seek to revise the state of the international system to their advantage. However, when they find themselves in an offense-advantage system in which they cannot distinguish between an offensive posture and a defensive posture, conditions can force them to behave like aggressor states. Status quo powers find themselves forced to engage in arms races during peacetime and

---

to preemptively attack others during a crisis because they cannot ascertain the intentions of others with absolute certainty and they do not expect to emerge victorious from a conflict in which their enemies strike first. In contrast, when they find themselves in a defense-advantage system, they will build up defensive military forces (if such forces can be distinguished from offensive ones) and prepare to receive their adversary’s first blow. Besides this, such a world exhibits greater crisis-stability than an offense-advantage one, since the incentives to conduct a preemptive surprise attack on the other power diminish, especially for status-quo states.

Over the past several years, the Department of Defense and each of the armed services have released new documents detailing their cyber strategy. To begin with, the official DOD strategy document details three primary missions for American cyber forces: to defend DOD networks from attack, to defend American non-defense networks against attack, and to support military operations and contingency plans. The majority of the documents detail a defensive strategy, emphasizing the need to absorb an enemy blow while maintaining the ability to operate in cyberspace. For example, the document explains “The Defense Department must be able to secure its own networks against attack and recover quickly if security measures fail ... If and when DoD detects indications of hostile activity within its networks, DoD has quick-response capabilities to close or mitigate vulnerabilities and secure its networks and systems.”28 Similarly, documents such as the Navy’s Information Dominance Roadmap primarily focus on maintaining present day capabilities, such as the ability to command, control, and coordinate forces and provide assured access to the electro-magnetic spectrum, even in contested environments. These concepts imply a primarily defensive and status-quo mindset. The publicly available information on the distribution of the cyber force supports the assertion that the United States has chosen to adopt a defensive posture. Of the 133 teams composing the Cyber Mission Force, Cyber Command has tasked 81 teams to defensive missions, 27 teams to offensive missions, and an additional 25 teams to missions that support both offense and defense.29 While these personnel do not constitute the totality of the cyber personnel available for national security purposes, such a distribution would be broadly consistent with the United States’ position as a status-quo power upholding global responsibilities while facing no immediate military threat.

Despite the official line, there are indications that American cyber experts and strategists hold divergent views on the nature of the cyber domain. Some make their differences quite explicit. For example, former Deputy Secretary of Defense William Lynn, writing one of the earlier significant cyber pieces in Foreign Affairs, simply states that “In cyberspace, the offense has the upper hand ... the US government’s ability to defend its networks always lags behind its

---
29 http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy
adversaries’ ability to exploit US networks’ weaknesses ... In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind a Maginot Line of firewalls or it will risk being overrun. Cyberwarfare is like maneuver warfare, in that speed and agility matter most.” Additionally, Lynn clearly believes that in the cyber domain the offense holds a substantial advantage over the defense in cost-effectiveness. As he explains, “cyberwarfare is asymmetric. The low cost of computing devices means that US adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to US military capabilities. A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States’ global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target.” Lynn ultimately concludes that the United States should primarily seek to reduce this disparity by researching ways to improve its defenses and enhancing its ability to react quickly to an attack. However, he derives these conclusions not from a belief that the cyber domain as presently constructed will reward such an approach but rather from the idea that cyber as a man-made domain can be altered in order to change its fundamental nature.

Beyond this, there are indications that military personnel see the world differently from the civilian political appointees in the Department of Defense. For example, General Keith Alexander made clear that he did not expect his organization to take a defensive posture during his testimony before the US Senate Committee on Armed Services in 2013. As he explained, “I would like to be clear that this team, this defend the Nation team, is not a defensive team; this is an offensive team that the Defense Department would use to defend the Nation if it were attacked in cyberspace.” Consequently, some of the Cyber Mission Force teams, and particularly the National Mission Teams, would appear to have less of a strictly defensive purpose than their description would imply. Additionally, the tone and focus of General Alexander’s public statements broadly implies a more aggressive mindset as compared with documents such as the 2015 DoD Cyber Strategy, which adopt a more defensive minded tone. Similarly, service-specific strategies tend to emphasize offensive measures to a greater degree than equivalent DoD documents. For example, the US Navy Information Dominance Roadmap includes a section specifying ways the Navy will “Disrupt/Deny/Defeat Red Fires”. Among other things, it seeks ways to “Develop a cyber exploitation and attack capability to predict and defeat cyber attacks before they occur, to include preventing adversary weapons launch by defeating

31 Ibid, 98.
‘weapons on the rail’ or in the silo.”33 Although it is not clear what this would entail for particularly destructive cyber attacks such as SQL injection vulnerabilities, Cross-Site Scripting attacks, or buffer-overflow exploits, it clearly demonstrates an interest in developing ways to preemptively attack enemy cyber capabilities as a means of defending friendly forces against attack.

Finally, even advocates of a defensive cyber posture largely concede many critical points regarding cyber’s offensive nature. To support its operations, the Department of Defense depends on an amalgamation of networks that span the globe.34 The DoD only operates a small fraction of these systems itself; instead, most are run by private sector corporations in the United States or a variety of organizations internationally. Many of these actors lack the capacity and skill to adequately secure their systems and the DoD lacks the mandate to protect much of this critical infrastructure on their behalf. Even if it gained the legal authority and access to attempt to protect this network, the vast attack surface would quickly prove impossible to defend under any realistic resource constraints.35 In light of these difficulties, the 2015 Department of Defense Cyber Strategy recommended focusing on protecting only the most critical pieces of infrastructure from cyberattack. Unfortunately, it is unclear that even this objective can be accomplished. Far from expecting that the United States will maintain dominance in cyberspace akin to its capabilities in other domains, the report expects that US forces may not be able to rely on cyber capabilities and must prepare to do battle without them. It explains, “Since the end of the Cold War, however, a younger generation has grown increasingly more accustomed to an environment of connectivity … In the face of an escalating cyber threat, the lessons of the previous generations must now be passed down … Organizations must exercise and learn to operate without the tools that have become such a vital part of their daily lives and operations.”36 Such an attitude hardly exudes confidence in the recommended defensive measures.

Similarly, most current American strategy documents concede the cost-advantage to the offense in cyberspace. As Joint Publication 3-12 on Cyberspace Operations states, “Information and communications technology (ICT) and other advanced technologies are used by a wide range of state and non-state actors, and represent an inexpensive way for a small and/or materially disadvantaged adversary to pose a significant threat to the US. The application of low-cost

35 Ibid, 13
36 Ibid, 4-5
cyberspace capabilities can result in disproportionate effects against a technology-dependent nation or organization. This provides actors who could not otherwise effectively oppose the US using traditional military forces with an asymmetric alternative.”

The 2015 DoD Cyber Strategy broadly agrees, arguing that even American enemies who lack the indigenous cyber talent to field top-tier cyberwarfare programs could potentially buy weapons on the black market at a substantially lower cost compared to the resources needed to purchase advanced conventional military equipment.

All in all, it seems clear that American policy makers of all stripes, even those that advocate a defensive posture for American forces in cyberspace, believe that the cost structure of cyber favors the offense.

**Solving the paradox of American cyber strategy**

Overall, US beliefs about cyber warfare appear to be caught in a paradox. American strategists would like to achieve dominance in cyberspace akin to American dominance in other domains. More importantly, they must protect the United States against a devastating strike, either targeting the homeland or forces which have been forward deployed to protect American interests and allies. The dual defeats of Pearl Harbor and 9/11 loom large in this mindset, with much of American cyber literature emphasizing the need to avoid cyberattack equivalents to these historical “bolt-from-the-blue” attacks. Unfortunately, neither an offensive nor a defensive posture seems to offer much hope of accomplishing these goals. American enemies can choose their target from a vast attack surface of critical nodes which means that any defensive strategy shapes the competition in their favor. However, the lack of counterforce targeting for many types of cyberattacks means an offensive strategy offers few guarantees either. Jack Snyder, in his book *The Ideology of the Offensive*, has documented the risks of this situation. As he explains, “Rationalization is also likely when the strategist has no acceptable options – this is, when any strategy would almost certainly involve an unacceptable sacrifice of some key value. In practice, decision makers in this situation tend to adopt risky strategies, but in rationalizing this choice, they also tend to overrate the probability that their strategy will succeed. In other words, people see the ‘necessary’ as possible.”

This condition poses a substantial risk to the future evolution of American cyber doctrine. When forced to design and implement a risk-acceptant strategy, war planners typically must make simplifying assumptions in order to develop a “successful” plan. Often, these assume away unpredictable adversary responses and reduce the margin for error during the execution of the plan. Unfortunately, events in the real world rarely allow for such

---


suppositions. In war, the enemy always gets a vote; unanticipated occurrences can catastrophically disrupt plans which allow no margin for error. Similarly, advances in technology and military professionalism have yet to banish friction or the fog of war from the battlefield. Commanders ignore these lessons of history at their peril.

In order to solve these policy conundrums, the United States must take several steps. First and foremost, the United States will need to create a cyber strategy that reduces the scope of its problem to something it can solve and tilts the competition with its adversaries to pit its strengths against their weaknesses instead of the other way around. The current cyber strategies, both for the Department of Defense as a whole and for individual services, largely consist of a set of goals and subgoals disconnected from any specific foreign policy situation or adversary. Although the gaps in these documents suggest that much of American cyber strategy remains classified, too much of American strategic thinking in the modern era has confused declaring a number of objectives with actually developing an actionable strategy. Instead, true strategy identifies key opportunities to be seized and obstacles to be overcome in order to win a competition against a competitor. After all, every organization acts under conditions of scarcity; not every desirable goal can actually be accomplished against a particular competitor or with the available resources. At the same time, the competitor’s organization has difficulties and weaknesses of their own that a skillful strategist can exploit. By focusing strategic thinking within the context of a particular competition or at the very least a grouping of competitors sharing similar characteristics, American cyber strategy can focus on specific opportunities and actions as compared with formulating a plan of action against an amorphous and idealized foe.

In addition to devising competitor-specific strategies, the United States also needs to do more to understand the unique characteristics of the cyber domain. Much of the current analysis of cyber weapons views them through the lens of established concepts and technologies. For example, Keith Alexander laid out his vision for the future of Computer Network Attack in the document Warfighting in Cyberspace. In it, he advocates for shifting perspectives about cyberwarfare from merely conducting influence operations to considering it simply another type of weapon akin to a bomb or artillery shell. Cyberspace operations documents from the individual services have expanded upon this theme. Such comments mirror the initial reaction of the armed services to previous revolutionary changes in the nature of warfare brought about by the influence of information technology. For example, Dima Adamsky has described how American leaders were slow to comprehend the revolutionary changes brought about by the introduction of precision guided munitions in the 1970s, incorrectly perceiving the new weapons as simply a somewhat better bomb. While the United States has often led the world in introducing technological innovations, its conceptual and doctrinal frameworks often lag behind its newly introduced

capabilities. Indeed, American adversaries such as Russia and China often comprehend the true potential of American inventions more completely than their American creators do. To correct for this, the United States should establish new organizations within each of the services to examine the impact of the evolving nature of warfare in the near future, or approximately a fifteen- to twenty-year time horizon. These officers would focus on developing new concepts of operations just as engineers focus on designing new weapon systems. Although an organization the size of the United States military will hardly transform its theoretical constructs overnight, by bringing together innovative personnel and providing them with an institution to amplify their efforts, the United States could speed up the full integration of new capabilities within its forces as well as completing some of the preparatory work to compete with more agile adversaries that do not share its attachment to legacy platforms and standard operating procedures.

Finally, the United States will need to invest in technologies and mechanisms that will act to reduce the advantage provided to the offense in cyberspace and improve crisis stability. Many of these investments are already underway. Although the hardening of critical infrastructure and building of resilient systems provide a good start, the United States will need to avoid tactical constructs that would aggravate its security dilemma. For instance, Stephen van Evera’s work on the origins of the First World War explores how perceived “windows of opportunity” interacted with doctrinal beliefs regarding the primacy of offensive action to create strong incentives to launch a preemptive strike. Some technical characteristics of cyberweapons can create similar incentives. To take one example, maintaining persistent access to a compromised enemy system can prove difficult. Consequently, if a cyberweapon has been emplaced during a crisis period, concerns will grow over time that enemy action may nullify the weapon prior to its employment and decision makers may find themselves facing a “use it or lose it” dilemma. Ensuring persistent access to enemy networks could help to reduce these worries, especially against potential opponents such as China or North Korea that possess an enhanced ability to isolate their national networks compared with the United States. Additionally, the United States may need to analyze prospective cyberweapon designs to determine their flexibility during a potential crisis scenario. Inflexible weapons or tactics can aggravate crisis situations by eliminating potential paths to de-escalation or forcing go/no-go decisions at a phase of the crisis that might not otherwise warrant one. By evaluating these characteristics at the design phase, engineering teams can build in features to make these weapons more adaptable than they might otherwise design for.

All in all, experts everywhere find themselves still in the early stages of understanding the full impact of cyberweapons on the future of warfare. To date, there has never been a recorded fatality due to the use of a cyberweapon and cyberattacks have played only a minor supporting

---

role in world conflicts so far. However, many theorists see great potential in cyberwarfare. Just as the United States once relied on nuclear weapons and information-enabled weapons to provide it with the first and second offsets, other powers today are now searching for offsets of their own to overcome American dominance of conventional warfare utilizing the descendants of the dominant weapon systems of the Second World War. The Chinese, among others, believe that cyberweapons present them with the greatest potential to achieve this goal. Only by carefully studying the capabilities and intentions of its opponents can the United States devise a strategy to defeat them in the most effective and efficient manner.

**About the Author**

James Ryseff is a technical lead at Google. He has been a software engineer for the past fourteen years and has previously worked as a Development Manager at SAP and as a Software Development Engineer at Microsoft Corporation. He received his B.S in Computer Science from the University of Illinois at Urbana-Champaign and his M.S. in Security Studies from Georgetown University’s Security Studies Program. The opinions expressed here are his own and do not reflect those of any of his current or past employers.

The report was authored by a non-CSIS-affiliated scholar. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).