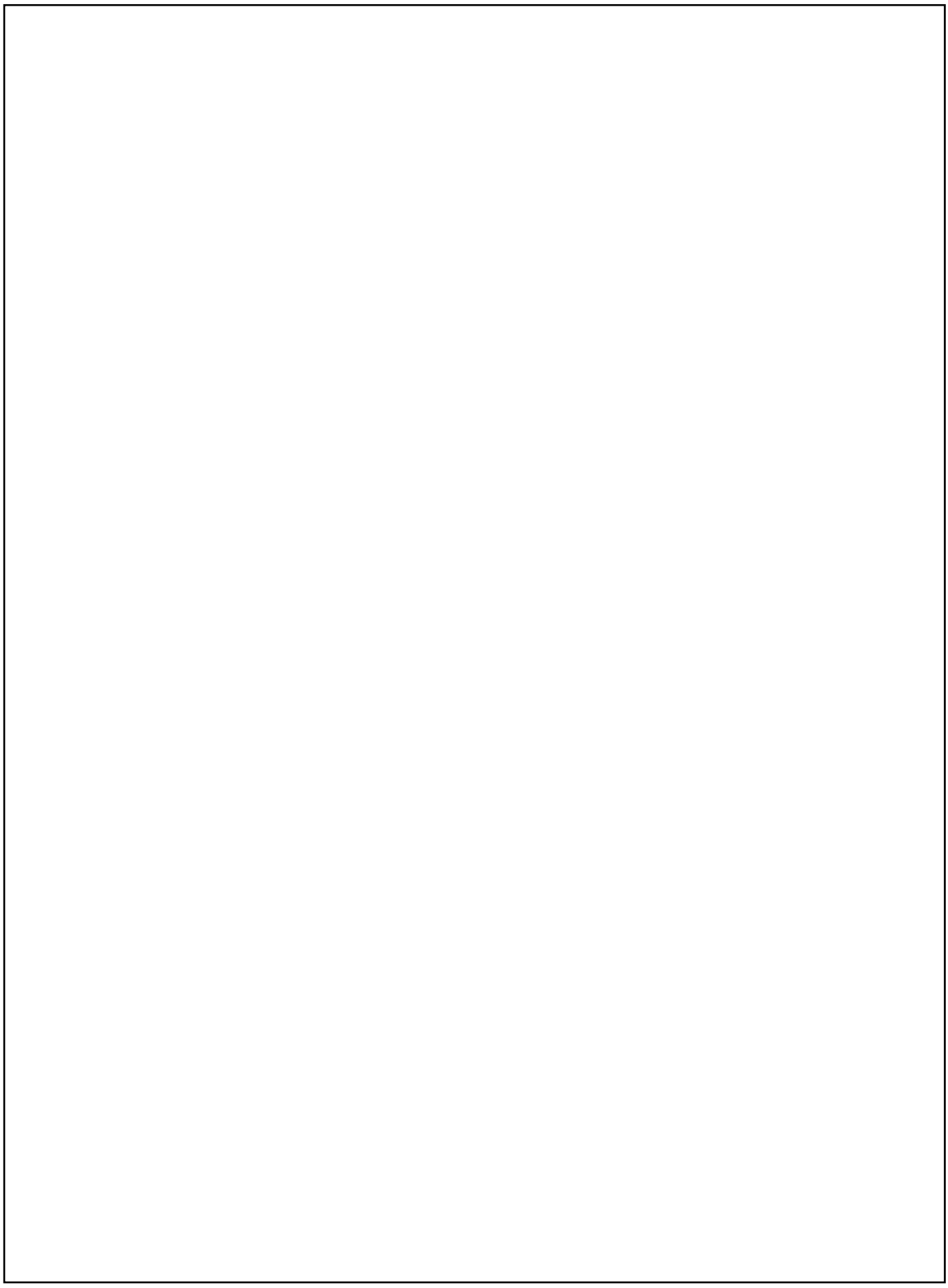

Strategic Stability and Cyber Warfare: Challenges and Implications

Majid Mehmood

Introduction

Deterrence continues to be an important feature of international political life regardless of the conditions of polarity in the international system. The origin of strategic stability concept can be traced back to the Cold War deterrence configuration in the bi-polar relations of two nuclear armed super powers in terms of Mutually Assured Destruction or MAD. MAD implied that the correlations of nuclear forces are such that it discourages first strike thereby preserving the mutual vulnerability of the physical state. Thus nuclear deterrence is the core concept upon which the foundation of strategic stability is built or at least sought by states.

It is important to mention that deterrence in isolation is a fragile basis of strategic thinking and it should be placed within broader framework of policy objectives. Nuclear armed states have an interest in preserving their nuclear capabilities against a number of contingencies that can potentially erode their nuclear potential. The challenge to deterrence and strategic stability is to be analyzed in the traditional framework of analysis.

Cyber domain is increasingly becoming a major concern in regards to warfare in general and strategic stability in particular. However, it is a complex phenomenon and the complexity emanates from factors such as varying magnitude of network attacks and its impact, problem of attribution, varying doctrinal perceptions among states and proportionality and nature of responses.

Cyber conflict and strategic stability are traditionally discussed as separate fields of international relations and military strategy research and practice. There is however an overlap between cyber-conflict and strategic stability due to a number of factors. First is the Command, Control, Communication, Computer and Intelligence (C4I) aspect of nuclear command and control. Hardened and secure

C4I system is life line of nuclear and conventional command and control center and their survivability.

Second, offensive cyber-capabilities when coupled with conventional operations have the potential to create escalation dominance in the initial phase of conflict, thereby forcing an opponent to think of escalating conflict to regain strategic advantage. Although the problem of attribution remains central to response dilemma associated with cyber-attacks, nonetheless it can create a perception within the opponents that a large scale cyber-attack on defense networks and electricity grids could be a prelude to a conventional conflict. Strategic stability therefore could become more vulnerable and fragile as a result of large scale cyber-attacks.

This paper explains the relationship between strategic stability and cyber-warfare, its likely implications for strategic stability and the challenges in cyber domain.

Cyber Space and Cyber Warfare

The digital world has brought both opportunities and threats for human race. Since information technology and the internet have developed to such an extent that they have become a major element of national power and cyber-war has become an important aspect of cyber domain as nation-states are arming themselves for the cyber battle space. Many states are not only conducting cyber-espionage, cyber-reconnaissance and probing missions; they are creating offensive cyber-war capabilities, developing national strategies, and engaging in cyber-attacks with consistency.

Cyberspace consists of computer networks in the world and everything they connect and control via cable, fiber-optics or wireless. From any network on the Internet, one should be able to communicate with any computer connected to any of the Internet's networks. Thus, cyberspace includes the Internet plus lots of other networks of computers including those that are not supposed to be accessible from the Internet. Some of those private networks look just like the Internet, but they are, theoretically, separate. Other parts of cyberspace are transactional networks that do things like sending data about money flows, stock market trades, and credit card transactions. Thus, cyberspace is composed of computers, along with servers,

routers, switches, fiber-optic cables, and wireless communications that allow critical infrastructures to work.

The accelerating rate of advances in technology, combined with an increasingly unstable geopolitical environment, makes the current period perhaps the most promising for broad, dramatic shifts in the military competition since the era between the two world wars[1]. The interwar period 1919-1938 saw the advent of combined-arms, mechanized air-land operations (blitzkrieg), the displacement of the line of battle at sea by fast carrier task forces, the rise of long-range strategic aerial bombardment, and the introduction of integrated air defense networks[2]. Post World War II witnessed the introduction of nuclear weapons, as well as cruise and ballistic missiles, which triggered another fundamental change in the character of warfare.

The First Gulf War of 1991 witnessed the advent of precision-guided weapons warfare which resulted in the increase in the effectiveness of air power. That war also saw the onset of a rapid expansion in the US military's reliance on space systems for a wide range of missions, from intelligence, surveillance, and reconnaissance (ISR), to target acquisition and tracking, guiding munitions to their targets, and providing battle damage assessment[3]. In response, we have recently seen the Chinese military test several types of anti-satellite (ASAT) weaponry. Viewed from this perspective, cyber-warfare is a facet of "precision warfare" and a competition in space but arguably the least understood form of warfare[4].

Based on what has been explained as cyber space earlier, Cyber warfare can be defined as "actions by nation-states and non-state actors employing cyber-weapons to penetrate computers or networks for the purpose of inserting, corrupting, and/or falsifying data; disrupting or damaging a computer or network device; or inflicting damage and/or disruption to computer control systems[5]". Cyber war can involve engaging in acts of espionage, criminal activities, and economic warfare. It can also include actions designed to support military operations at the tactical and operational levels of war, as well as independent operations designed to achieve strategic effects[6].

What constitutes a "catastrophic event" in the cyber space is an important discussion as well. Webster's dictionary defines catastrophic event as "a momentous tragic event ranging from extreme misfortune to utter overthrow or

ruin." In terms of nation states we can interpret "utter overthrow or ruin" as the end of a regime or even the disintegration of a state or loss of its sovereignty. Perhaps this is why policy-makers are faced with warning of the potential for "catastrophic" destruction or consequences without providing any specifics.

In the context of massive nuclear exchange, the effects would be instantaneous and long term for the targeted societies. On the other hand, Cyber-attacks can be executed at high speed but their effects may not be felt for days and months due to instant counter measures that are in built within the cyber related systems of the targeted states.

Due to this reason, a catastrophic event in cyber space will be defined with variation and not by a standard conventional framework. This formulation will have to include the intensity, nature and scope of cyber-attacks coupled with what comes after the cyber-attacks as these linkages combined will be critical factors for determining the thresholds of strategic stability.

Cyber Warfare and Strategic Stability

There are two interlinked aspects that connect cyber-warfare with strategic stability. First is the potential impact during or before crisis trajectory and second is the impact on the command and control aspect of nuclear operations.

Cyber warfare could exacerbate instability during a crisis trajectory due to the following reasons:

First, the effects of a cyber-attack tend to be short-lived[7]. Once the victim realizes that one of its networks have been penetrated, affected systems can be purged, restored, secured or worked around in just hours or days[8]. Because the interval between a cyber-attack and the defender's recovery can be short, fully exploiting any advantage that is gained by the attacker requires that it be followed promptly by a conventional strike, even in circumstances that would otherwise favor observation and defensive preparations. These places the conventional forces in the classic dilemma of move out or lose out after a successful cyber-attack. Knowing this, the side that suffers a cyber-attack could decide that it is imprudent to wait and see whether a strike by the enemy's conventional forces will follow, and may instead act preemptively.

Secondly, cyber-attacks are difficult to duplicate after they have been made the first time, for they involve guile, not force. An attack's discovery informs defenders that they had neglected to secure their networks adequately. As most cyber-attacks exploit some piece of vulnerable computer code, they can reveal the source of weakness, allowing the code to be patched or routed around, and the problem is solved. The difficulty of duplicating cyber-attacks supports the logic of early use and prompt exploitation in order to maximize their effect. Put differently, if a cyber-attack causes the defender to improve its defenses, it is best carried out early, by surprise, and with the intent of maximum effect before defenses are improved.

Thirdly, the effects of a cyber-attack may be difficult for both the attacker and the defender to assess. The attacker will know what was supposed to go wrong, but not necessarily whether it actually did so (particularly if the defender isolates the attacked network in order to diagnose and repair it). The ambiguity of results may, again, weaken the effectiveness of cyber warfare. In the context of a crisis in which both sides have reason to fear that the other might strike first, such ambiguity is more likely to be interpreted darkly by the side suffering the attack. This means that any detected cyber-operation could lead to conventional war, regardless of whether the attacker intended it to do so[9].

Fourthly, and related to the previous consideration, a network penetration carried out for the purposes of cyber espionage may be hard to distinguish from one carried out to degrade a network in preparation for a conventional armed attack[10]. Penetrating some networks (such as that of an integrated air-defence system) is likely to indicate preparations for war, penetrating others (such as those of C4ISR or supply systems) might be no more than spying. The difficulty of distinguishing the opening stage of a cyber-attack, such as network penetration, from cyber-espionage may cause defenders to interpret cyber-espionage as a precursor to war, rightly or wrongly, and to react accordingly. The side that has been attacked may be disinclined to give its adversary the benefit of the doubt, particularly during a crisis.

Fifthly, a failed cyber-attack may go unnoticed by the target. It could be stopped by the network's firewall and look no different than thousands of other failed penetration attempts. Or it may succeed in penetrating the firewall and infecting

the host, but give commands that do not have effects that are clear enough to be noticed. The likelihood that such failure will go unnoticed by the target reduces one risk of cyber-attacks, and thus potentially lowers the cost of carrying them out. By contrast, most failed kinetic strikes are more easily detected, meaning that the aggressor risks trying, failing and being retaliated against anyway.

Overall, the nature of cyber warfare is such that its effects, as well as its effectiveness, may be ambiguous and limited. Although not inherently destabilizing in the classic sense that counterforce capabilities sometimes are, a cyber-attack unaccompanied by a kinetic strike could nonetheless trigger armed conflict, either because the attacker is under time pressure to exploit its temporary effects or because a defender interprets it as a precursor to conventional attack. Moreover, if an attacker is motivated to engage in cyber warfare at all, it may be motivated to launch a major attack – to give it its best shot, rather than give the enemy a chance to improve defenses. Assessing how serious this danger is requires a closer look at the ways in which cyber-warfare might be used, and the different paths between it and conventional war leading to the nuclear level.

Nuclear Command and Control

Nuclear weapons must be incorporated into systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The weapons and their C4ISR systems must be protected from attacks, which are both kinetic and digital in nature. In addition, the decision makers who have to manage nuclear forces during a crisis should ideally have the best possible information about the status of their own nuclear and cyber-forces and command systems, about the forces and C4ISR of possible attackers, and about the probable intentions and risk-acceptance of possible opponents.

The task of managing a nuclear crisis demands clear thinking and good information. But the employment of cyber weapons in the early stages of a crisis could impede clear assessment by creating confusion in networks and the action channels that are dependent on those networks[11]. The temptation for early cyber-preemption might "succeed" to the point at which nuclear crisis management becomes weaker instead of stronger.

The appeal of non-nuclear systems, including cyber-weapons, for prospective attackers rests in part on their putative capacity for mass disruption combined with precise lethality. On this very point, Russian Deputy Prime Minister Dmitri Rogozin has warned that information weapons are becoming first-strike weapons against enemy's political, military, and industrial centers[12]

Conclusion

Information technology may make it possible for states to inflict meaningful, although not necessarily decisive, damage against the networks and command systems of an opponent in the early stages of a conventional or nuclear war. The aspects that make information warfare work, including the (at least) temporary ability to prevent discovery of the attack or the identification of its source, conspire against the clarity of information needed to defuse a nuclear crisis or to terminate a nuclear war. Improvements in reconnaissance-strike complexes may make possible the reliable destruction of nuclear targets by conventional means. The same technologies could improve nuclear targeting, too, thereby compromising the assured survivability of retaliators and first strikers.

Majid Mehmoodis a
CISS Associate Research Officer

ENDNOTES

[1]Williamson Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period* (Cambridge, United Kingdom: Cambridge University Press, 1996). For an overview of military revolutions, see Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," As quoted in the paper titled "Cyber warfare: A Nuclear Option?" by Andrew Krepinevichwww.csbaonline.org/wp.../08/CSBA **Cyber Warfare** For Web 1.pdf

[2] Ibid

[3] Andrew Krepinevich, "Cyber warfare: A Nuclear Option?" 2012, Center for Strategic and Budgetary Assessment Report, accessed January 02 2015, www.csbaonline.org/wp.../08/CSBA **Cyber Warfare** For Web 1.pdf

[4] Ibid

[5]Richard A. Clark, *"Cyber War: The Next Threat to National Security and What to Do About it",* April 10, 2012, P.70

[6] Ibid

[7] Based on the study of the impact of stuxnet attack on the Natanz enrichment plant, it can be said that the duration of the worm attack was limited and focused only on the destruction of centrifuges. Once the attack was identified, counter measures were taken to secure the control system spinning centrifuges. David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?"December 22, 2010.Accessed

December 26, 2014.http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf,
[8] Ibid

[9] David C. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability", 25 July 2014, http://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc
[10] Ibid
[11] Stephen J. Cimbalaa, "Cyber War and Deterrence Stability: Post-START Nuclear Arms Control", 25 July 2014, Comparative Strategy Journal, http://www.tandfonline.com/doi/pdf/10.1080/01495933.2014.926727, Accessed 31 December 2014
[12]Rogozin, cited in IlyaMaksimov and Sergey Kuksin, "Russia Will Not Be a Bystander in the Arms Race," RossiyskayaGazeta, June 28, 2013, in Johnson's Russia List, no. 122, (July 5,2013), available at davidjohnson@starpower.net