

Principles of Cyberwar

**Lieutenant General Sunit Kumar, AVSM (Retd)[®] and
Associate Professor (Dr) Anurag Jaiswal[®]**

“Principles are a code of conduct, but not an absolute one”¹

- George Kennan

Abstract

For decades military strategists have studied and evolved the ‘Principles of War’. Drawn from the long history of armed conflicts, these guidelines encapsulate the things that often lead to battle field successes. They reflect the accumulated wisdom of conventional war fighting. In this regard, some authors have said that cyberwar is also the continuation of kinetic war by other means. However, it is not; the two are quite different. One might say that they are checkers and chess – which only look the same because their terrain is the same and some of the pieces have the same name. It is, therefore, a great challenge to those military and cyber security experts who apply the rules of conventional war to the cyberwar². Cyberwar does have rules, but they are not the ones we are used to – and sense of fair play is certainly not one of them because of the inbuilt plausible deniability in cyber war. This article is not intended to be a comprehensive list but rather an attempt to suggest ‘Principles of Cyberwar’ to initiate a general discussion and dialogue on this subject³.

Introduction

In the history of warfare, the first person credited with principles to regularise methods of fighting should be SunTzu. Principles

[®]**Lieutenant General Sunit Kumar** served as DG IS (Army HQ) from 2011 to 2014 before his superannuation. An alumnus of DSSC, HC and NDC, he served in various staff, command and instructional appointments in the Army. He has recently completed his PhD in ‘Cyber Warfare – Challenges and Options for India’s Defence’.

[®]**Dr Anurag Jaiswal** is an Associate Professor with the Department of Defence Studies, Meerut College, Meerut (U.P) since 2003. He has done his post-graduation in Defence and Strategic Studies from University of Allahabad and his Ph.D from CCS University Meerut (U.P) in 2007.

Journal of the United Service Institution of India, Vol. CXLIX, No. 617, July-September 2019.

which he advocated, such as “know your enemy and yourself and in a hundred battles you will never be defeated”, “strike where the enemy is not prepared, take him by surprise” and “avoid the solid and strike the weak”⁴ are still articles of faith for modern strategists. A hundred year after the demise of ‘Napoleon the Great’, who elicited dread in the British both during life and after death; a British General by the name of JFC Fuller induced five principles of directing modern wars. All of the West’s principles of modern warfare have descended from these. This is because, from the beginning of the Napoleonic wars to the time prior to the Gulf war, apart from the continual increase in lethality and destructiveness, there was no essential change in the nature of war itself.

The digital revolution brought about a new type of war: Cyberwar. Its impact was seen vividly in the First Gulf war. Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles.⁵ Since IT and the internet have developed to such an extent that they have become a major element of national power, cyberwar has become the drumbeat of the day, as nation-states are arming themselves for the cyber battle space. Cyber space is increasingly used as a theatre of conflict as political, economic and military conflicts are even more often mirrored by a parallel campaign of hostile actions on the internet. The principles of kinetic warfare as we know them are well documented, but they are not fully applicable to cyber warfare. Differences between cyberspace and the real world suggest some additional principles; this article therefore, proposes some new principles of cyber warfare.

Principles of War: The Conventional View

Before the battle of Kalinga, when the ‘Maurya Empire’ was at its peak, the emperor is reported to have proclaimed, “*Vijay hi ek-matra yudh ka sidhant hai* (Victory is the only principle of war)”. A similar quote by Winston Churchill, too, is significant, “Victory at all costs, victory despite all terror, victory, however long and hard the road may be; for without victory, there is no survival.”⁶ Overarching principles immutable through the ages, however, have a problem, they do not factor in the tremendous changes which have occurred due to technology and provide no direction to the strategists who plan war. Hence, greater detail is required by specifying the principles which give direction to reach the ultimate principle of victory in the digital

technology era. For decades military strategists have studied and refined what they call 'the principles of war'. Drawn from the long history of armed conflict, these guidelines encapsulate the things that often lead to battlefield success. They are not immutable laws; bold commanders sometimes ignore them and still win. But they reflect the accumulated wisdom of war fighting.

The principles of war as taught in the schools of instruction of the Indian Army, are based on Clausewitzian traditions. The principles that constitute the present doctrine are⁷:

- (a) Selection and Maintenance of Aim.
- (b) Offensive Action.
- (c) Concentration of Force.
- (d) Economy of Effort.
- (e) Flexibility.
- (f) Cooperation.
- (g) Security.
- (h) Surprise.
- (i) Administration.
- (j) Maintenance of Morale.

Principles of Unrestricted War — Chinese “Unofficial, Official” Views

Unrestricted Warfare which in Chinese translates to literally “warfare beyond bounds” is a book written in 1999 by Colonels Qiao Liang and Wang Xiangsui of the Peoples Liberation Army. In 1989⁸ they had stated that “the first rule of unrestricted warfare is that there are no rules, with nothing forbidden”.⁹ Elaborating this idea, the authors asserted that strong countries would not use the same approach against weak countries because “strong countries make the rules, while rising ones break them and exploit loopholes[...]”. The concept of unrestricted warfare is closer to British strategist Liddell Hart’s concept of ‘Grand Strategy’ than to German Strategist Ludendorff’s ‘Concept of Total War’. Not only do the non-kinetic aspects take precedence over the kinetic dimension, but the modus operandi is not based upon the all-encompassing mobilisation

of a nation's resources. The occurrence of the 'Revolution in Military Affairs' — the emergence of technologies so disruptive that they make existing concepts obsolete and necessitate a rethinking of how, with what, and by whom, war is waged has altered the dynamics of war. The First Gulf war showed that war is still brutal, however, the mass carnage of World Wars I and II was missing. War is still disruptive but not in a kinetic manner. In warfare of the era of globalisation, all participants are interconnected and interlocked. This makes unavoidable that people, places and economies far removed from the battlefield will be affected. This is obvious because the concept of a "battlefield", a "frontline" or a "rear area" all get diluted in "unrestricted warfare". The increasing incidence of non-state actors, low intensity conflict, nuclear weapons which make conventional war prohibitive and globalisation has set on course events which change the way wars are increasingly being fought. This has set in motion the first change of course since the dawn of history where "bloodless" wars in cyber space which indirectly attack the enemy can take place. This has laid a new track for war in the next century and given rise to principles with which professional military people are unfamiliar. No principle can rest on a platform of a different era waiting to collapse.

As per the authors of Unrestricted Warfare, the concept of "empty basket", (of military thinking) relies upon the principle of utilising the non-changing to deal with the myriad changes¹⁰. The key to whether or not victory is won in a war is nowhere else but in "what things you are able to pack into this basket"¹¹. On the specifics, the authors put forward as principles to pursue a "beyond limits combined war"¹² as principles of unrestricted warfare, quite different from the conventional principles of war. They state these as under:

- (a) Omni-directionality.
- (b) Synchrony.
- (c) Limited Objectives.
- (d) Unlimited Measures.
- (e) Asymmetry.
- (f) Minimal Consumption.
- (g) Multi-dimensional Coordination.
- (h) Adjustment and Control of the Entire Process.

Views of Western Writers

The Western World view of Clausewitz conceptualises war using enunciation and upholding of aim, mass and manoeuvre among other principles in a state-on-state kinetic war for a political intent. Contrarily, Sun Tzu's Eastern World conceptualises war, focusing on the criticality of intelligence and deception to defeat the mind of the enemy, knowing that relationships matter most in the strategy of war.

However, the great challenge for military and cyber security professionals in the present era much removed from Clausewitz and Sun Tzu is that incoming attacks are not predictable and current strategies for prevention tend to share the flawed assumption that the rules of conventional war extend to cyberspace as well. Cyber warfare does have rules, but they are not those we are used to and a sense of fair play is certainly not one of them. Moreover, these rules are not intuitive to the generals, who are versed in fighting the conventional wars. That's the problem because cyberwar won't be waged with the informed participation of much of the technology sector.

Stuart H Starr of the National Defence University, USA has written a chapter in *Cyber Power and National Security*¹³, which focuses on initial efforts for developing a framework for theory of cyberpower. He discusses the merits of a revised set of modernised principles of war for the 21st Century, as suggested by Charles Dunlap in 2006, vis-à-vis their relationship to the traditional principles¹⁴. These are :-

- (a) **Perceived Worthiness.** Morale: is it worthwhile to risk one's life?
- (b) **Informed Insight.** Sense-making, cognitive, surprise.
- (c) **Strategic Anchoring.** Concentration on and prominence of the offensive.
- (d) **Durability.** Incorporate security into plan; depends on logistics.
- (e) **Engagement Dominance.** Incorporates and simplifies manoeuvre; improve/oppose surprise.
- (f) **Unity of Effect.** Draws on unity of command, reinterprets economy of force mass, manoeuvre.

(g) **Adaptability.** Presupposes flexibility but does not mandate simplicity.

(h) **Culminating Power.** Power needed to attain satisfactory closure at a given level of conflict.

Cyberwar is the continuation of kinetic war by plausibly deniable means. May be we can state that cyberwar is kinetic war by other means; well it's not; the two are quite different. One might say they are as checkers and chess – which only look the same because their terrain is the same and some of the pieces have the same name.

Suggested Principles of Cyber War

Do the principles of war, hitherto circumscribed as they are due to lack of familiarity and first-hand experience of non-traditional war-milieu, coupled with hi-tech destitution in reference to cyber domain, continue to be valid ? This article states that they are not valid. Hence, a new list of principles of cyberwar are required. These principles — fairly enthused by what are listed and described in Unrestricted Warfare — are distinct from the conventional principles of war. An understanding of irregular warfare fosters a rudimentary knowledge of cyber warfare. By highlighting how irregular warfare and cyber warfare are similar and providing the critical framework for using IW principles to approach, define and integrate cyberspace operations across all domains and services, military planners can begin to understand how cyber power can increase the effectiveness of the nation's military cyber force.¹⁵

Sun Tzu's principles that steer non-kinetic cyberspace operations are still important guides. The most advantageous way to subdue the enemy is to attack the mind of the commander(s) or better still, that of the political leader(s) at the helm. Cyber war provides the most effective means for that – gathering intelligence through cyberspace and exploiting deception in cyberspace. Therefore, the new set of principles of cyberwar proposed are:-

- (a) Pursuance of National Interests.
- (b) Mobilisation, Motivation and Morale.
- (c) Unity of Command and its Well-defined Chain.
- (d) Technological Supremacy.

- (e) Network Knowledge and Cortex Centricity.
- (f) Surprise, Stealth and Subterfuge.
- (g) Organisational Agility and Power to the Edges.
- (h) Synchrony and Integration.
- (i) Spontaneity in Response.
- (j) Situational Understanding.
- (k) Security of Centres of Gravity.
- (l) Global Cooperation

Conclusion

The new principles of war are no longer using armed forces to compel the enemy to submit to one's will, but are using all means, including armed forces or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests. Though some military writers have attempted to apply the traditional principles¹⁶ of war to cyberwar, but it seems more useful to start with a blank sheet of paper to begin discussion and debate about what should constitute the principle of cybeware. The principles of conventional war emerged from centuries of experience. Cyber is new, so its parameters and implications will be dynamic for quite some time and will evolve with usage and experience.

Endnotes

¹ American diplomat and historian. He was best known as an advocate of a policy of containment of Soviet expansion during the Cold War.

² Tarah Wheeler, "In Cyberwar, there are no Rules", illustration by Kyle Hilton for Foreign Policy, September 12, 2018, <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/>

³ R.C. Parks, and D.P. Duggan, "Principles of Cyberwarfare," September/October 2011, pp. 30-35, vol. 9

⁴ Qiao Liang and Wang Xiangsui, Unrestricted Warfare, (Beijing: PLA Literature and Arts Publishing House, February 1999), Accessed <https://www.c4i.org/unrestricted.pdf>

⁵ John Arquilla & David Rondfelt, Cyber War is Coming, https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf

⁶<<http://www.brainyquote.com/quotes/quotes/w/winstonchu138231.html#d2OYWgw ykh>

⁷ Indian Army Doctrine, n. 2, ch.3

⁸ Qiao Liang and Wang Xiangsui

⁹ *ibid*

¹⁰*Ibid.* n 7, ch. 4

¹¹ *Ibid.*

¹² *Ibid.*

¹³ *Ibid.*Chapter 3 “ Towards a Preliminary Theory of Cyberpower” in n.2, ch 2, pp 43-88

¹⁴ *Ibid*, pp. 56-57

¹⁵ Frank C Sanchez, Weilun Lin and Kent Korunka, “Applying Irregular Warfare Principles to Cyber Warfare”, 01 Apr 2019, NDU press

¹⁶ Samuel Liles, J. Eric Dietz, Marcus Rogers and Dean Larson, “Applying Traditional Military Principles to Cyber Warfare.