

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/321824579>

Is Clausewitz Compatible with Cyber?

Article · August 2015

CITATIONS

0

READS

1,149

1 author:



[Jared L. Ware](#)

United States Military Academy West Point

46 PUBLICATIONS 10 CITATIONS

SEE PROFILE

Is Clausewitz Compatible with Cyber?

By

Jared L. Ware

The theories proposed by Carl Von Clausewitz almost 185 years ago maintain relevance based on their applicability relating to the rise of non-state actors and the increasing relevance of cyber operations in the context of modern warfare. Clausewitzian theory is useful in the Computer Age and continues to offer insights to some of the most consistently experienced issues in modern warfare. The recent release of the Department of Defense (DOD) Cyber Strategy is predicated upon the tenacious adherence to a comprehensive strategy, a topic to which Clausewitz devotes a significant amount of attention. Another area of interest for success in cyber warfare is defining the proper mix of joint Cyber Mission Forces (CMF) to fight and win the nation's future wars (DOD Cyber Strategy). Clausewitz again provides valuable insights by analyzing the relationship between the branches of service in the context of battlefield efficacy. Some may contend that with the exponential proliferation of technology and non-state actors that Clausewitz and his theories lose relevance, and this may apply in the context of legacy, kinetic-based warfare. However, Clausewitz will continue to influence future generations of American military practitioners simply from the standpoint that his theories remain rooted in the very nature of warfare. Additionally, nation-states and non-state actors will continue to operate across the cyber domain, where the changing definitions of terms such as "lethality" and "magnitude" are factors in a new form of warfare.

The 2015 DOD Cyber Strategy discusses how the United States, a 21st century *Nation-State*, will prosecute the Global War on Terror. One of the most significant realities addressed in

the new strategy is the recognition of agile non-state actors and their use of technology to advance their causes. The basic premise is that the nation's adversaries are increasing severity and sophistication of the cyber threat to U.S. interests, to include DoD networks, information, and systems (DOD Cyber Strategy). Although Clausewitz focused his strategic theories around the concept of a *Nation-State*, his thought process remains valid in the current operating environment. A *Nation-State* at war with illusive non-state adversaries requires the strategic quality of perseverance to ultimately bring its enemies to their knees. Clausewitz understood that only great strength of will can lead to the objective (Howard and Paret, 193). Even if non-state actors, who do not necessarily fear retaliation, are to deploy a cyberattack, which causes serious physical damage to unprotected infrastructures in stronger states, retaliation is likely (Jacobson, 13). It is reasonable to assume that the nation on the receiving end of a cyber attack will enlist the support of allies and use various means of retaliation if their collective strategic interests are at stake.

The new cyber strategy recognizes that the achievement of the proposed objectives will take five years, and that perseverance remains a central component to achieving victory. A central component of cyber warfare is achieving the proper mix of joint forces, particularly after a decade plus of sustained combat operations. Every service continues to tout the advantages of their specific capabilities, weapons systems, and relevance in taking down "the bad guys" in an effort to showcase their respective advances in cyber warfare. Clausewitz offers valuable insights to building the optimum force structure in the context of a relative operating environment. He states that if one could compare the cost of raising and maintaining the various arms with the service each performs in the time of war, one could end up with a definite figure

that would express the optimum equation in abstract terms (Howard and Paret, 286). In essence, Clausewitz is writing that force structure requires an honest, thorough review based upon the metrics and realities of warfare, a review that is rooted in complementary conventional and cyber force structure.

To their credit, the services have rapidly developed their respective cyber commands and a joint command has been established to ensure interoperability and a linkage to the national command authority. However, the services must go beyond the “copy and paste” approach of transitioning existing subordinate capabilities and putting “Cyber” in front of the title of the higher headquarters. This will suffice in the interim to establish a cyber warfare culture, but it will not achieve an optimal solution for cyber warfare capabilities. For the military, this requires a shift from simply adapting capabilities based on the direct action, kinetic-based “Thunder Runs” of the previous Gulf Wars and the deliberate, nation-building counterinsurgencies in Afghanistan and Iraq to understanding a new strategy, and eventually innovating new capabilities rooted in perseverance, persistence, and practicality in the cyber domain.

The Department of Defense can take advantage of Clausewitzian logic as it refines the joint cyber mission force mix with respect to the National Security Strategy, the new DOD Cyber Strategy, and military events over the past decade. Instead of focusing solely on the resurgence of conventional doctrine and large-scale kinetic weapons systems, the entire military-industrial complex requires a realistic, disciplined approach in its efforts to achieve a balanced and credible force structure. Although the current operating environment still requires a mix of conventional weapons systems from all services, it also requires strategic foresight with respect to asymmetric threats, non-contiguous adversaries, and non-state actors as these relate to cyber warfare.

Senior level analysts and planners should evaluate the existing cyber threat, review the past few years' metrics, and provide senior defense officials with an unbiased force structure assessment that includes a credible mix of joint, interoperable cyber capabilities complemented by interagency, intergovernmental and multinational cyber assets.

Some modern military practitioners may contend that Clausewitz and his theories are invalid or obsolete in today's cyber operating environment, especially with respect to advanced technology. As pointed out by Williamson Murray and Macgregor Knox, the "technological utopians" are free to reject Clausewitz as an unworldly nineteenth-century figure whose Kantian philosophical framework held no place for technological change (Murray and Knox, 178). However, Clausewitz's writings withstand the complexity of the Computer Age and all of the Cyber technology it presents. Even supercomputers equipped with the finest software and most advanced algorithms cannot model all of the mathematical permutations and combinations of unpredictable warfare, or the Clausewitzian "fog of war" condition so often referenced by military historians. Moreover, one of the problems Clausewitz articulated was that a lack of information would limit the ability of commanders and politicians to effectively act (Greathouse, 30), particularly those enamored by the latest in cyber hardware and software and those with decision-making cycles that require the comparison of metrics derived from such systems. Perhaps Clausewitz's greatest contribution to the profession of arms is recognizing war as a human endeavor, and that technology is an enabler of warfare, not its panacea, even in context of cyber warfare.

The theories of Carl Von Clausewitz provide valuable insights to 21st century military planners, practitioners and observers of warfare. *On War* is as relevant to the battle against non-

state actors equipped with advanced technology as it was to 19th century nation-states advancing the fight with horse cavalry. U.S. military practitioners should continue to study and understand Clausewitz's theories and reflect upon the merit of his postulates. In the 20th century, Clausewitz's theories withstood two world wars fought on the European continent as well as a "Cold War" waged between the world's two greatest superpowers. For military planners now and in the future, the rigorous study, practice, and reflection of Clausewitz's ideas will provide guideposts to victory in today's environment and ultimately towards winning wars in cyberspace.

Works Cited

Addington, Larry H. The Patterns of War Since the Eighteenth Century. Bloomington: Indiana University Press, 1994.

Department of Defense Cyber Strategy, April 2015.

Greathouse, Craig B. *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? Cyberspace and International Relations*, Springer-Verlag Berlin Heidelberg, 2014.

Howard, Michael and Peter Paret. Carl Von Clausewitz: On War. Princeton: Princeton University Press, 1976.

Jacobsen, Jeppe T. *The Cyberwar Mirage and the Utility of Cyberattacks in War - How to Make Real Use of Clausewitz in the Age of Cyberspace*. Danish Institute for International Studies Working Paper 2014:06. Copenhagen, 2014.

Knox, MacGregor and Williamson Murray. The Dynamics of Military Revolution 1300-2050. Cambridge: Cambridge University Press, 2001.

Jared Ware is a Lieutenant Colonel in the United States Army. He recently served as the Division Engineer and Senior Protection Cell Coordinator for the 82nd Airborne Division, Fort Bragg, North Carolina. His next assignment as an instructor in the Department of Geography and Environmental Engineering at the United States Military Academy, West Point, New York.