Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

What Did Clausewitz Have To Say About "Sybre"?

Applying Clausewitzean Principles to Disrupt the Cyber Threat Advantage through Counter-Value Actions in All Domains

CCHS Commentary - By John Mills - September 2018

Introduction

"We have plenty of Cyber Rommels ready to perform their cyber pincer envelopment. What we need are more Cyber Eisenhowers and Marshalls to articulate the strategy for victory and securing the long-term peace in Cyber."[i]

Carl Von Clausewitz (1780 – 1831) has had an enduring effect and impact on the study of conflict, nation state relationships, military organization, and leadership. His observations[ii] have proved timelessly applicable since his era.

The epoch of Cyber is now upon us and a cursory overview shows again that Clausewitz's thoughts have application. In many ways, he foresaw and explained the same dynamics national security and industry leaders are struggling with today. With the rise of expansionist, soft totalitarian, imperial-like China, a return of aggressive Russian adventurism, and violent extremism filling in the blank spaces, a new era of world affairs is upon us. One that requires grand strategic thought and calculus.

Although by title this paper may appear to be focused upon the cyber domain, the intent however is to communicate a full spectrum, asymmetric, American strategy that encourages the initiative of action in all domains.

The purpose of this is twofold – to allow the American instruments of national power to gain momentum and the initiative in world affairs, and secondly to put the threat actors on their heels in contested domains such as Cyber. In the cyber domain, the offense has the initiative and the momentum. The cyber defensive interests are being overwhelmed.

Currently much of the thought in the cyber domain focuses solely on response actions in the cyber domain: the threat hits the US in cyber – the US hits back in cyber. This is simplistic and ensnares American and allied interests in a struggle of attrition.

Instead, American national security and business structures must look holistically across all domains and instruments of national power and not constrain themselves to limiting cyber response actions to the cyber domain. It has been shown through events like the OPM breach[iii] that the defenders are woefully behind in the decision making and action loop.

In the cyber domain and era, the OPM breach and the response were not U.S. cybersecurity's finest hour due to the lag in time from detection to decisive decision making. A response in cyber to a cyber act may be appropriate, but a non-cyber response may also be appropriate and more impactful.

Establishing the peace in cyber cannot be established by just focusing on cyber. National security and industry leaders must treat the cyber struggle as a counter-value (vice counter-force) situation.

In this way they can send an unambiguous strategic message on the nation state's resolve for holding a threat actor's centers of gravity at risk. Only by this method will the behavior of threat actors change.

Applying Clausewitzean Tenets to Regain the Initiative in Cyber

Clausewitz espoused several key principles that are applicable in any period of friction and competition among nation states and non-nation state interests. This paper will use Clausewitz's principles as captured in US Joint Military Doctrine.[iv] These principles should be used to harness precious US government and industry efforts in a resource-constrained environment by ensuring maximum effect at the right place at the right time.

This paper addresses a few of the more pertinent Clausewitzean tenets as exemplars and presents clear and actionable courses of action. Some are new ideas, some are re-invigorating existing ideas that have not been aggressively implemented.

1. Articulate the Objective

Clausewitz was clear on this – articulate an objective and stick with it.

In Cyber the principles are the same; establish clear, defined, and attainable national policies (coordinated with international partners) and enforce coordinated executive branch plans, policies, and execution through a robust and timely inter-agency process.

National leaders need to identify and communicate objectives and red-lines, or the threat will continue to fly deep and wide into their networks, while defenders wallow and agonize in the complexity of the situation.

Example starting points on establishing Objectives in Cyber:

1. Declare the sovereignty of American Government data and US Corporation data and networks and also the willingness to use counter-value, asymmetric actions to protect these.

2. Hold nation states responsible for Cyber Crime emanating from their territory. Target their cyber personalities by name, associate them with their national government counterparts who are often facilitating their actions by omission or commission, and aggressively indict and prosecute.

3. Create a multi-lateral, secure environment for networks and systems – a Cyber NATO inclusive of Pacific and Middle East Partners.

4. Cyber Re-Flagging – Similar in concept to tanker re-flagging of the 1980s[v]; through declaratory policy or statute, communicate a clear statement of cyber protection for American and Partner nation commercial interests and a clear willingness to protect these interests. Information sharing, indemnification for defensive actions, and the unfettered access of international partners to American tools and capabilities would be part of this.

2. Take the Offensive

This Clausewitzean tenet is clear and highly applicable to the current cyber situation - seize the initiative and maintain the momentum. A defensive crouch to shield oneself from cyber blows is just that – a defensive crouch.

In international conflict or aggressive negotiations (or at least in frictional situations), if you aren't winning, you are losing. This is where a re-introduction of the Great Game aspect of world affairs is in order – use light touch, strategic offensive moves to maintain the initiative and momentum, and force the threat into reactive mode. Let the threat guess where and when the next move will be.

Actions must demonstrate a real or potential ability, and, even more importantly – ***national resolve*** - to hold adversary centers of gravity at risk. By demonstrating this resolve and ability, adversaries will then be forced into the same non-advantageous defensive, reactionary crouch.

There are several immediate low-resource, "offensive" actions that can help take the pressure off the cyber domain. Policy on offensive actions in cyber is still relatively immature[vi] and second and third orders of cyber effects are still unpredictable. That being said, re-taking the "offense" in all domains will allow us to re-posture and get out of our defensive crouch in cyber:

1. Strongly support, through statute, the ability of private sector firms to offer protective and active defense services to sectors under assault. In some ways, this means deputizing private sector firms for lawful actions in cyber. This would free up US Government resources to conduct oversight and advisory roles and focus on the real high-end threat.

2. Aggressively use Law Enforcement authorities to nimbly respond and inflict cost on adversaries. Reserve cumbersome Title 10 authorities for the right time and place, meaning for situations where visible deterrence is needed, such as to keep open world waterways, or to discourage overt aggression or adventurism by competitor states or their proxies (like Iran is conducting in several locations). Overt and covert Title 50 actions can be used or held in reserve as the wild card factor. Law Enforcement capacity should be significantly increased to police the

intellectual property domain and stem the tangible flow of GDP from the US to foreign interests that do not create wealth but abscond with it.

3. Disrupt foreign military sales of aggressor nations – use different instruments of national power to disrupt their sales and the supportability of their platforms. Also take advantage of this domain by re-asserting American offerings as reliable and capable alternatives.

4. Actively enforce vacuum (i.e. weakness or vulnerability) management – maintain enough presence and deterrence to protect your vacuums and hold threat vacuums at risk. The threat also has vacuums – so national security decision makers must maintain an economy of force presence in their own vacuums and if nothing else, show a willingness to encroach upon others' vulnerable vacuum areas. Just the specter of willingness to move upon these unguarded threat vacuums has immense effect.

3. Rely on Maneuver, Not Attrition

Clausewitz encouraged a conflict of maneuver instead of attrition. His dictum directed movement of forces to a more advantageous position. This is where we accelerate the Great Game aspect of cyber conflict.

In cyber, the US Government cyber phalanx[vii] is unwieldy and slow to maneuver and respond. And often the focus of US Government response efforts is counter-force, not counter value. When a threat actor shows the ability to reach into a US Government Agency network and take data, then an asymmetric response should be part of the response option menu.

Through several decisive maneuvers, the US Government can lead a coalition of partners in low cost maneuvers that will take pressure off vulnerable centers of gravity and force competitors to re-allocate resources and decision-making capacity to address these moves.

Such actions could include the following – all would also send strategic messages of American resolve to peer or near-peer actors:

1. Actively stage material in the South China Sea area with the demonstrated end intent of building sovereignty just like other nations. Just like China can create an island and mythical sovereignty, so can the US. An expansion of the float on/float off capability of the Military Sealift Command[viii] and sharing of these resources with partner nations can help support this maneuver.

2. Foreign nations are actively involved in the expansion and operation of the Panama Canal and alternatives in Nicaragua. A renewed and re-invigorated, grand and strategic, worldwide American international program of engagement should strive to replace these competitor nation states with American alternatives. In many geographic areas, American

presence or at least a communication of American interests has disappeared. This seeming lack of American interest or at least curiosity must be reversed.

3. Just like Chinese interests are establishing oil platforms in the Gulf of Mexico, allied interests should conduct exploration for oil, undersea manganese nodules, and other rare earth metals in contested littoral waters.

4. Aggressively resurrect the capacity to build and sell diesel submarines to foreign partners. This is a critical strategic enabler and strategic message.

5. Resurrect defunct multi-lateral alliances such as SEATO[ix] and CENTO. Also explore new alliances in Europe, Asia, Africa, and South America to outmaneuver the overtures of Russia and China.

4. Adopt Unity of Command

Clausewitz advocated a clear chain of command and placement of your entire force under the command of a single entity.

In cyber, there is a similar need for unified focus and leadership of all elements of national power. In the Executive branch this is challenged by Department and Agency activities that overlap numerous congressional oversight, authorization, and appropriation committees. The US Government works most effectively when the threat fits nicely and neatly into one US Code (i.e. Title 10, Title 18, Title 50, etc.).

The challenge with Cyber is that it spreads across many US Codes and therefore the US Government is paralyzed by inter-agency coordination to establish jurisdiction, objectives, and courses of action. Some beginning points of change to facilitate better unity of command could include the following:

1. Address, through statute, the utter inability of Departments and Agencies to pivot in current fiscal years to urgent cyber and cybersecurity requirements. Current budget processes in the Departments and Agencies essentially establish a three-year cycle from initiation of requirements to arrival of funds, to implement proposals. DoD has NDAA 1206/2282 Authorities – this should be further clarified so that funds can be rapidly re-programmed for urgent cyber, space, national security and other requirements.

2. Greatly simplify the acquisition processes for urgent cybersecurity requirements for the US Government. This would indemnify contracting officers and programs managers from legal challenges to contract awards, and through statute would establish the legally sufficient threshold of a bare minimum of documentation required under a certain annual dollar ceiling for urgent cyber and cybersecurity requirements.

Right now, the metric for the legal teams engaged in discovery proceedings in award and contract disputes is the number of linear feet of contract documentation to review. Nothing will move fast (especially contract awards) when this is the metric. DIU and the Commercial Solution Openings statute-based procedures are a good start.[x]

3. Establish a Leahy Amendment for Cyber where recipients of U.S. Foreign Aid must verify and certify that they do not allow cyber-criminal or terrorist cyber activity within their sovereign territory.

4. Address broad export control reform. This has broad bi-partisan support. At one time, American national security exports were used in a grand-strategic way, to foster alliances and partnerships. Unfortunately, this has now devolved into a highly bureaucratic exercise that drives away nations considering engagement with the US and frustrates long-standing US partners. The world market should be flooded with American options – the American options should not be locked up in a vault, secure from the access of partners and potential partners. There have been recent positive trends in this area, but these must be accelerated even further.[xi]

Summary and Conclusion

Clausewitzean thought is applicable in the modern era of cyber. Before American cyber strategy is further established, a clear consideration of these timeless tenets across all of the domains of conflict must be considered. Cyber thrusts can be parried with cyber and non-cyber responses in a grand strategic way that can re-establish the initiative and pull the liberal, democratic republic nation states out of their passive cyber defensive crouch.

---

[i] *Unattributed Cyber Quote of the Day 2018* (Mobile Phone App).
[ii] Andrew Holmes, *Carl von Clausewitz's On War: A modern-day interpretation of a strategy classic* (London: Infinite Ideas, 2010)
[iii] Brian Krebs, *Congressional Report Slams OPM on Data Breach,* KrebsonSecurity website. Accessed, March 31, 2018. https://krebsonsecurity.com/2016/09/congressional-report-slams-opm-on-data-breach/
[iv] *Joint Publication 3-0, Joint Operations*, August 11, 2011. Department of Defense website. Accessed January 30, 2016. http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf Appendix A.
[v] United Press International, *Kuwaiti tankers reflagged with Stars and Stripes,* July 21, 1987. UPI Archives. Accessed March 21, 2018 https://www.upi.com/Archives/1987/07/21/Kuwaiti-tankers-reflagged-with-Stars-and-Stripes/5770553838400/
[vi] Angelyn Flowers and Sherali Zeadally, "US Policy on Active Cyber Defense," *Journal of Homeland Security & Emergency Management*, June 2014, Vol. 11 Issue 2, p289-308.

Accessed January 30, 2016,
http://eds.a.ebscohost.com.ezproxy.umuc.edu/eds/pdfviewer/pdfviewer?sid=cfc041fa-ce5a-43bf-bae1-e30b587eca90%40sessionmgr4001&vid=1&hid=4202.
[vii] "The Phalanx", no date. *Ancient Greek Battles*. Accessed January 30, 2016. http://ancientgreekbattles.net/Pages/90087_PhalanxHistory.htm
[viii] "NASSCO floats out first AFSB variant of MLP", November 10, 2014. *Marine Yellow Pages*. Accessed January 30, 2016. http://www.marineyellowpages.com/index.php/nassco-floats-out-first-afsb-variant-of-mlp.
[ix] U.S. Department of State Office of the Historian. "Milestones 1953-1960 Southeast Asia Treaty Organization (SEATO), 1954", no date. Accessed January 30, 2016. https://history.state.gov/milestones/1953-1960/seato
[x] Rick Docksai, "DIUx Releases Guide For Faster, Less-Costly Technology Acquisition". DoD News, Defense Media Activity. November 30, 2016. https://www.defense.gov/News/Article/Article/1016994/diux-releases-guide-for-faster-less-costly-technology-acquisition/
[xi] Aaron Mehta, "Two key industry groups hope now is the time to push a major change to the defense export process". Defense News. June 1, 2018. https://www.defensenews.com/industry/2018/06/01/trade-group-intensifies-push-for-security-cooperation-strategy/

John Mills has 35 years of experience in the National Security Community and is retired from both the U.S. Army as a Colonel and as a civilian from the Department of Defense where he last served as the Director of Cybersecurity Policy, Strategy, and International Affairs. He has served in the Cold War, Peace Dividend, War on Terror, and Post-War on Terror periods. He is Principal Director and Partner at CA2, LLC and also teaches graduate level Cybersecurity and National Security Policy and Strategy at a major University.

About Us

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

Website http://cchs.gwu.edu **Email** cchs@email.gwu.edu **Twitter** @gwcchs