ISN
ETH Zurich

21 August 2014

Some Principles of Cyber Strategy

Although cyberspace has existed for decades, the strategic principles of cyber-warfare have not yet been devised. In beginning to do so, John J. Klein believes that similarities between the cyber and maritime domains suggest that the thought of Sir Julian Corbett should be used as inspiration.

By John J. Klein for ISN

We humans have a habit of allowing the latest technological marvels to overwhelm our more critical strategic sense. - Colin S. Gray

Although cyberspace has existed for a few decades, strategic thought on cyber warfare lags significantly behind the technology that enables it. Much of this condition has to do with the mistaken belief that past strategic thought is not applicable to this man-made domain. Yet because of the importance of the Internet to the global economy and national security, it is critical to understand the fundamental principles of cyber strategy. Without such strategic principles, resources may be squandered on ill-conceived endeavors, while failing to achieve the intended national security objectives in the cyber domain.

The cyber domain

The cyber domain, or cyberspace, has been defined by Andrew Krepinevich as the world’s “computer networks, both open and closed, to include the computers themselves, the transactional networks that send data regarding financial transactions, and the networks comprising control systems that enable machines to interact with one another.” As such, the cyber domain utilizes expansive lines of communication involving a global network, along with hubs of activity at server farms or network hardware locations. Cyber activities involve international commerce and finance, social media, information sharing, and more recently, military-led activities. Cyberspace is not the sovereign territory of any one state, but incorporates both global commons that can be uncontrolled and widely distributed hardware located within sovereign territory. Additionally, cyber operations directly impact and are interrelated with the land, sea, air, and space domains.

Despite the ubiquitous nature and importance of the cyber domain, very little has been written regarding its strategic significance and importance relative to the land, sea, air, and space domains. Nevertheless, as was the case initially with the air and space domains in conducting warfare, analogy to other forms of warfare can be beneficial when developing strategic principles. In fact, using historical analogy to develop cyber strategy may be unavoidable. When considering potential candidates for developing a cyber strategy through analogous comparison, the maritime domain seems strikingly similar.

The maritime domain involves human activities on the seas and oceans of the world, including the interrelationships of science, technology, industry, economics, trade, politics, international affairs, communications, international law, social affairs, and leadership. Additionally, the maritime domain involves global lines of communications that are predominately not controlled by sovereign states, along with widely dispersed maritime assets, hubs of activity at ports, and congested communications at choke points. Because cyber and maritime operations seem to share many strategic-level considerations, maritime strategy may be useful in developing cyber strategy through historical analogy.

Principles of cyber strategy

In this effort to develop a maritime-inspired cyber strategy, the work of Sir Julian Corbett (1854-1922) will be used as a framework. Corbett was a British theorist and strategist who was renowned for his 1911 work *Some Principles of Maritime Strategy* and is acclaimed by many historians as Great Britain's greatest maritime strategist. What follows are some strategic principles for cyber warfare using over 200 years of maritime strategy for inspiration.

Cyber is tied to national power

The elements of national power have been said to include diplomatic, information, military, and economic considerations. The cyber domain directly impacts the last three of these elements, and therefore, cyber activities are linked to national power. First, cyber activities typically involve the sharing of data and information. This may include communications to convey an intended message or affect the views of others. Second, for many countries, including the United States, cyber is a critical element of today's military planning, and it is thought that future hostile actions by potential adversaries will include either defensive or offensive cyber actions. Cyberspace being the realm of military-led action is exemplified by the establishment ofU.S. Cyber Command and the People's Liberation Army Unit 61398. Third, the cyber domain is used extensively in finance and trade. Keith Alexander, former Director of the National Security Agency and Commander of U.S. Cyber Command, said that the ongoing cyber-thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history.

Cyber operations are interdependent with other operations

Cyber strategy should support an overall national strategy, just as land, maritime, air, and space sub-strategies ostensibly do. Additionally, cyber activities traverse the land, sea, air, and space domains. Service members across all the armed services routinely rely on cyberspace to plan for and facilitate the execution of military operations. In many cases, military operations would be significantly degraded if there were a denial or disruption of cyber connectivity. Because cyberspace is extensively used in the conduct of land, sea, air and space operations, cyber activities and effects should be fully considered when conducting operations in any of these domains. Although military personnel conducting cyber operations will need the support of the other military branches in working towards common wartime objectives, the other military branches likewise need the support of cyber educated forces to be as effective as possible.

Cyber Lines of Communication (CLOCs)

The inherent value of the cyber domain is the utility and access it provides. This utility and access are enabled through cyber lines of communication (CLOCs). Generally stated, CLOCs are those lines of communication in cyberspace used for the movement of data and information. By ensuring access to its own CLOCs, a state can better protect its national interests, including information, economic, and military activities. Because access to and use of cyber is vitally important, the primary objective of cyber strategy is to protect and defend one's own CLOCs while limiting the enemy's ability to use its. As with maritime communications, lines of communication in cyberspace often run parallel to an adversary's and may at times even be shared with him. Because of this, an adversary's cyber communications frequently cannot be attacked without affecting those of both parties.

Offensive strategy

Offensive strategy in cyberspace is called for when political objectives necessitate wresting or acquiring something from the adversary. Such a strategy may be needed to protect a state's interests in cyberspace and ensure access to CLOCs. Based upon Corbett's writings, offensive strategy is the more "effective" form of warfare, and application of this thinking means offensive operations in cyberspace should usually be attempted by the stronger cyber power. Achieving decisive victory via cyber operations will prove difficult, so sensationalist terms such asCyber Pearl Harbor or Cybergeddon can be unhelpful when considering a fully developed cyber strategy.

In the cyber domain, it is important to remember that offensive action should have real-world effects and not just include network intrusion or manipulation of data and information. Any offensive cyber action should result in some physical asset being damaged or some service being denied with real consequences. Examples of offensive action include manipulating the operation of electrical power grids, opening the floodgates of dams, or prolonged denial of service to banking institutions. Furthermore, offensive cyber strategy should include the counter-attack. Such a counter-attack may include " hack backs " in response to an adversary's initial cyber-attack.

Defensive strategy

Defensive strategy, on the other hand, is called for when political objectives necessitate preventing the enemy from achieving or gaining something. Corbett believed defensive strategy to be stronger than offensive strategy. During wartime, he concluded that a defensive strategy should be assumed when one is weaker than the adversary, and a defensive strategy should be abandoned once one is able to pursue the offensive.

Because the primary purpose of cyber strategy is to ensure access to CLOCs, any suitable defensive strategy should support that objective. Therefore, measures that provide defense against cyber-attack, harden cyber systems against electromagnetic damage, or incorporate redundancy in mission critical systems are all suitable methods of supporting the goal of a cyber defensive strategy. It is noteworthy when considering defensive strategy that China has developed its own network of companies behind a " Great Firewall," in order to screen incoming content and disconnect from the worldwide Internet if needed.

Dispersal and concentration

As Corbett argued in the context of maritime warfare, cyber warfare should emphasize flexibility between concentration and dispersal of its effects. Because cyber space is expansive and ever increasing, cyber strategy must address the method of employing and distributing systems, data, information, and effects to best protect national interests, while maintaining the ability to concentrate collective action when needed. This necessitates that systems, data, information, and effects be distributed, while linking together their " effectual energy " as if of a single will and with a common purpose. For cyber warfare, this means that cyber activities, in general, should be dispersed to cover the widest reaches of cyberspace, yet retain the ability to concentrate effects rapidly when needed. By dispersing systems, data, information, and effects, a variety of interests can be protected while facilitating defensive operations along many CLOCs. When action is necessary, cyber activities should concentrate their collective effects to defeat an adversary rapidly.

The recent actions of the group Anonymous are an example of this concept of dispersal and concentration, although there is no evidence of offensive action as the result. This “hacktivist” group is essentially composed of unidentified users from various Internet forums who collectively gather to conduct organized protests and other focused actions using cyber means. As a group, Anonymous works toward a common agreed upon set of goals, but all act independently toward achieving these goals.

Final thoughts

Some may argue that what has been presented here is purely an academic exercise using an antiquated strategy, with no utility in today’s reality of cyber operations. Such critics would likely note that maritime and cyber domains are very different, and therefore, Corbett is irrelevant. In contrast to maritime activities, cyber involves near simultaneous communications, prevalence of nonphysical effects and actions, rapidly advancing technology, greater opportunity for anonymous actions, more interdependence with the other domains, and still evolving understanding of its relative importance. Despite these differences, the similarities between maritime and cyber activities at the strategic level are sufficient to justify using Corbett’s work as a foundation to develop the principles of cyber strategy.

Through this analytical endeavor, one can see that cyber lines of communication, offensive and defensive strategies, and dispersal and concentration are useful ideas when contemplating cyber warfare strategy. Applying these ideas can facilitate the allocation of scarce resources to achieve national objectives and protect vital security interests. With continued access to cyberspace increasingly considered to be a critical requirement, a fully-developed cyber strategy is needed. Over 200 years of maritime history and strategy can usefully inform this effort.

John J. Klein is a Principal Analyst at Analytic Services in Falls Church, Virginia and writes frequently on national security, military strategy, and the Law of Armed Conflict. The views expressed in this article are solely those of the author and do not necessarily reflect those of Analytic Services or those of the United States Government.

Publisher

International Relations and Security Network (ISN)