Beyond Ones and Zeroes: reframing cyber conflict

Miguel Alberto Gomez
Center for Security Studies (ETHZ)

Introduction

Over the past decade, a steady stream of cyber operations has captured the imagination and stoked fears of the public at large. The possibility that a society increasingly reliant on cyberspace is at the mercy of actors capable of exploiting this dependency has been parroted across different quarters – from politicians, military leaders, and even academics. Since the worrying events in Estonia in May 2007, state-associated actions in cyberspace have grown increasingly complex – and with it our assumption of its strategic potential. Yet, interestingly, despite advances in their capabilities and increasing reach, most attacks have been viewed as strategically insignificant. The Distributed Denial-of-Service (DDoS) attacks against Estonian infrastructure, for instance, achieved little in coercing the Estonian authorities to shift their policies in favor of Russian interests. Similarly, the attributes associated with Stuxnet in 2010, despite being the first instance of physical damage resulting from cyber operations, did not dramatically hinder the Iranian nuclear programme. Ironically, it may have instead hardened Iranian resolve and jumpstarted their own cyber warfare program (Iasiello, 2013).

Inversely, lesser-known operations characterized by reduced sophistication and dramatic effect have resulted in noticeable gains. The BoxingRumble operation, part of the Snowden disclosures, demonstrated how the United States government had managed to discourage further Chinese espionage attempts against NIPRNET. Similarly, the OPM Hack did not result in any physical damage, but led to high-level talks between the American and Chinese governments to establish proper behavior in cyberspace (Jensen et al., 2016). With these interactions and their outcomes in mind, what are we to make of the state use of cyberspace? Is its strategic utility as espoused by its proponents during the first few years of the 21st century simply overrated? Perhaps not. While most of these events have not met their stated objectives, or at best have been tactical rather than strategic wins, one cannot discount their potential utility (Healey, 2016).

In so doing, this essay argues that perhaps the time has come to reorient our views with respect to the nature of cyber conflict. This essay proposes that two shifts are necessary before one can dismiss the strategic utility of cyber operations. First, we must begin to prioritize strategic considerations over technological determinism. The case of cyberspace heralding a revolution in interstate relations (e.g., war) is neither the first nor the last instance of technological enthusiasm. Similar sentiments were shared with the advent of airpower only to be firmly restrained through its continued use. Second, the notion of success in cyberspace must be framed in the context of heterogeneous threat perceptions. While there is no discounting the fact that cyberspace continues to make significant inroads across

... perhaps the time has come to reorient our views with respect to the nature of cyber conflict.

different societies and states, its valuation is by no means uniform. A cursory review of policy documents across states highlights different conceptualizations of cyberspace (Shafqat & Masood, 2016; Luiijf et al., 2013). This incongruity results in contrasting threat perceptions that, in turn, affect what one state would view as either victory or defeat. Borrowing from Wendt, it can thus be said that cyberspace is what states make of it.

Beyond Technology

The earliest discourse surrounding the strategic utility of cyber operations focused on the unique technological characteristics of the domain. Noting the "low cost of entry," difficulty with defense, and attributional challenges, proponents of what has been termed as the "cyber revolution thesis" believe that previous strategic thought does not and ought not to apply (Liff 2012). Given the rapid rise in the adoption of Information Communication Technologies (ICT) from the mid-1990s onward, one cannot be blamed for finding merit with this argument. Unfortunately, the historical record lends limited empirical support to such an astrategic view of cyberspace.

To begin with, most state-to-state exchanges in cyberspace have involved rivals. Maness & Valeriano have demonstrated that operations involving actors with enduring rivalries have nearly quadrupled since the year 2000. Moreover, issues such as territorial disputes and regime legitimacy have framed these interactions. It is of note that several of these actors have exercised a degree of restraint in cyberspace (Maness & Valeriano, 2015b; Maness & Valeriano, 2015a; Valeriano & Maness, 2013). Despite the notion that it is a relatively cheap domain to enter, these interactions are dominated by states with notable economic and military capabilities (Pytlak & Mitchell, 2016). Given the limited number of actors coupled with investment costs associated with cyberspace, the initial assumptions surrounding the domain are increasingly challenged. Yet, what about the question of defense? If highly capable actors are indeed utilizing cyberspace, shouldn't its use be maximized? To this end, it has been argued that the fear of escalation may be restraining overly aggressive behavior (Lawson, 2013). Despite the uncertainty in attribution, the small pool of participants involved and the issues surrounding most of these events minimizes the fog of uncertainty. So much so, that leaders like former US President Barack Obama have noted the possibility of a kinetic response to attacks in cyberspace.

Thus, the notion that cyber operations exist beyond the bounds of strategy is unfounded. As noted by Colin Gray, "cyber power is the ability to do something strategically useful in cyberspace" (Gray 2013). Yet, this requires one to establish a link between strategic interests and cyberspace. Unlike concerns surrounding the utility of cyber operations, this is far less contentious. Kuehl and succeeding scholars agree that cyberspace serves as an enabler for several instruments of national power that, in turn, serve strategic interests. Objectives including economic growth and military efficiency have been enabled by rapid developments in the domain (Kuehl, 2009; Starr, 2009; Nye, 2010). Consequently, the

ability to employ cyberspace to further these objectives while hindering those of a rival's determines the expected utility of cyber operations.

And, yet, a caveat exists. States do not have a standardized view of cyberspace (Giles & Hagestad, 2013). This implies that the level of support that cyberspace offers to specific instruments is inconsistent across states. For instance, while the United States may be able to alter the operations of critical infrastructure in China, this is far less worrying to the existing regime than if their adversary were to launch an information campaign through Iranian cyberspace. This view is strengthened if one were to observe that China's priorities seem to lie in censorship and content management rather than the overall security of their infrastructure (Lindsay, 2015). Ultimately, the expected utility of cyber operations is inherently linked to varying threat perceptions that emerge from differing conceptualizations of cyberspace.

Victory and Threat Perception

The question as to the exact nature of cyberspace continues to persist in this nascent field. Despite the unlikely appearance of consensus, cyberspace can be divided into two different conceptualizations. The first treats the domain as a technology-dependent space. This includes both the technology and the information flowing through it. Adherents of this view – also referred to as the "western consensus" – see in it an enabler of economic and political processes. Furthermore, this perspective is shared by states with liberal regimes that see in it a platform for spreading liberal-democratic values. In contrast, the second treats the domain as the space between technology where information exists. This encompasses the mind of individual users that participate in cyberspace. While this treatment also treats the domain as an enabler, it goes further by bestowing upon it societal and ideological value. Illiberal regimes, fearing the possibility of a counter-narrative from cyberspace challenging their legitimacy, often view cyberspace in this light (Rivera, 2015; Hare, 2012).

These two views, inclusive and exclusive, result in different prioritizations that influence threat perception. Most existing research into the utility of cyber operations fail to take this into account. This leads to the propagation of the belief of the astrategic nature of cyberspace (Gray, 2013). To demonstrate this point, the case of Stuxnet proves instructive. From the American perspective, their inclusive treatment of cyberspace could, in some sense, lead to the idea that Stuxnet was a victory (tactically). Since value is placed on the ability of cyberspace to support strategic interests (i.e. targeting Iranian centrifuges through cyberspace) would hinder their strategic goal of enriching Uranium. This logic is seen in other cases such as BoxingRumble wherein the disruption of the espionage network hindered the strategic objective of obtaining information.

On the Iranian side, however, a different mechanism is seen. While damage was inflicted on their equipment (albeit minimal), the lack of a significant response from the regime suggests that their valuation of cyberspace as a key enabler of their strategic interests vis-a-vis their nuclear program was weak. Although it may be argued that the limited damage could in part have mitigated a more vociferous response, their behavior in other instances is telling of their priorities in this domain. While the idea that Iran tightly censors the Internet is correct, this has not always been the case. During the

initial years of its introduction, the regime had been quite liberal relative to the region in allowing its citizens to use it as a platform for interaction and exchange. It was not until the appearance of rhetoric deemed subversive to the interests of the regime that steps were taken to regulate this space (Rahimi, 2003; Deibert & Rohozinski, 2010). It can then be argued that Iran perceives threats emanating from content rather than availability as a higher priority. In this respect, the Stuxnet operation was not viewed as a success on the part of the Iranians.

A Return to Strategy

Given the previously raised points, it would be foolish to haphazardly dismiss the strategic utility of cyber operations. While the historical record does not appear to adhere to the aspirations of its proponents, the utilization of cyberspace is by no means futile. Instead, special consideration ought to be made for how it is employed and its outcomes interpreted. First, one must acknowledge that cyber operations do not exist outside the bounds of strategy. Airpower, despite the notion that it would render rival state helpless and force them to one's will, had much less influence than originally proposed. Its critics have argued that context mattered in its exercises. Second, while it is indeed correct to suggest that the increasing ubiquity of cyberspace may render states more vulnerable, it does not do so consistently. Threat perception varies to the extent that, where one might view danger, another might deem it insignificant.

With the trend in state use of cyber operations showing no sign of abating, it becomes even more important to keep these points in mind. Promoting the view that cyber operations exist beyond strategy encourages its reckless use that could promote further instability in the international system. In contrast, understanding that it forms part of a state's toolbox that is to be applied carefully and at the proper time may lead to the emergence of behavioral norms that could stabilize this increasingly important domain.

Miguel Alberto Gomez is a senior researcher at the Center for Security Studies. He holds a Masters degree in International Security from the Institut Barcelona d'Estudis Internacionals. He has previously worked as a lecturer at both the De La Salle University and the College of St. Benilde in the Philippines and has worked in the Information Security industry for the past eight years. His area of research is centered around Cybersecurity. Specifically, he is interested in the strategic use of cyberspace as an instrument of national power as well the emergence of norms surrounding the use of this domain.