As governments become increasingly involved in cyberspace for military purposes, they tend to consider the cyber domain as critical part of their security strategies. This growing reliance on cyber assets calls for deeper investigation on the features of cyberspace as well as their impact on state rivalry. The paper draws from the insights of Offence/Defense Balance (ODB) theory to discuss whether competition in cyberspace may become an incentive to the use of force. In particular, ODB theory postulates that whenever defense is (or is held to be) more expensive relative do offense, states will have an incentive to act aggressively. Unfortunately, three features of cyberspace give offense an advantage over defense: the central place of vulnerabilities, the different pace of improvements for defense and offense technologies, the difficulty in attribution. The main conclusion of this argument is that the cyber-attacks in the future are likely to become more and more common.

*Andrea Locatelli, Catholic University Milan*
The way wars are fought has changed dramatically in the past decades. While the tip of the iceberg rests on fancy devices – like drones or the so-called smart bombs – a deeper and even more radical process is going on. As new technologies and military doctrines are continuously developed and revised war becomes an increasingly complex activity. This is hardly new, as witnessed by the nationwide efforts required by total wars like World Wars I and II. What is remarkable in our day is the (almost) unprecedented pace of innovations in military technology. To put it bluntly, some of today’s realities are yesterday’s sci-fi conjectures (and by yesterday we can consider a three-decade span of time). How all these changes are affecting war is still under debate and – as usually happens – this question has polarized analysts in two opposing camps: Conservatives vs Revolutionaries.

The rise of cyberspace as a domain of warfare is no exception. The impact of the Internet on military operations has brought analysts within both military circles and the academic community to discuss whether a digital revolution is occurring or not. As recognized most recently by Jon Lindsay, the Conservatives/Revolutionaries divide seems to follow the border between these communities: while most scholarly literature tends to dismiss the novelty brought about by the cyber-dimension, analysts and practitioners within the armed forces are more inclined to underscore its potential. Both camps

2 The literature on this topic has revolved since the early 1990s around the so-called Revolution in Military Affairs (RMA) concept. I have provided a more detailed overview in A. LOCATELLI, Tecnologia militare e guerra. Gli Stati Uniti dopo la Rivoluzione negli Affari Militari, Milano, Vita e Pensiero, 2010, pp. 23-64.
have forceful arguments to support their thesis, but their main weaknesses rest on the lack of evidence. Put it bluntly, whereas cyber-threats, illicit activities in cyberspace, are everyday’s business, none of them qualifies as a security threat, let alone an act of war. Nonetheless, as most militaries have come to depend on Information and Communication Technologies (ICTs), cyber-operations/commands have been developed and are now part of most advanced states’ armed forces.

It is too early to assess whether these offices are doomed to become the backbone of the fifth domain of war, or (like many other experiments before) they will live a short life. The point that needs to be discussed here is that as governments become more conscious of their capabilities (and vulnerabilities) in cyberspace, they will likely shape their own strategies accordingly. In other words, since strategy is the art of matching (political) ends and (military) means, the features of cyberspace as a potential military asset may have an impact on how states pursue their national security. In the following pages we will make some inference starting from the Offense/Defense Balance (ODB) theory. In the next section we will discuss the main tenets of this argument. We will then come to assess how cyberspace affects the ODB. Finally, section 4 will present the main conclusions.

The Offense/Defense Balance Argument

---

6 The only exception is the STUXNET virus that attacked the Iranian centrifuges in Natanz in 2009-2010.
7 See among others the ambitious Office of Force Transformation, established in October 2001 and closed just five years later.
Proponents and critics of the ODB hypothesis are mostly concerned with topical issues in international politics, such as the security dilemma\(^9\), war inception\(^10\), and escalation\(^11\). All these phenomena, the argument goes, can lead to opposite outcomes depending on a single variable: the (assumed) relative strength of offense over defense, and vice versa. Simply put, when attack and conquest are held to be easier than protecting a given target (being it a swath of land, a line of communication, or a military facility), ODB theory predicts as likely systemic outcomes an intense security dilemma, the possibility of major wars and the tendency to increase war aims. Even if the causal path can take many ways\(^12\), the logic of this argument is quite straightforward. When policymakers and strategists are convinced that the offender has an advantage over the defender, they will be tempted to perpetrate preemptive attacks. They will also be skeptical of their counterparts' intentions, as well as willing to take more risks in war.

On the other hand, when defense is easier than offense, states have more incentives to cooperate, embark on binding strategies and even engage in disarmament policies. To illustrate this point, in a seminal contribution Barry Posen argued that ethnic groups in failed states are less susceptible to the vicious logic of the security dilemma (thus preventing the outbreak of civil wars) if they can credibly show that their military forces are for defense only\(^13\). Or, more recently, Charles Glaser\(^14\) claimed that states seeking security have better chances of increasing their status without threatening other powers.

For heuristic purposes, the viability of this theory rests on the ability to spell out the causes of this balance. In a nutshell: since military power alone is too rough as a variable, what are the factors that solve the equation? Since the issue at stake is military victory, most authors turned to military technology as a catch-all.

---


\(^12\) S. VAN EVERA, *Causes of War...*, cit.


\(^14\) C. GLASER, *Rational Theory of International Politics...* cit.
explanation\textsuperscript{15}. The main line of argument is that throughout history technological developments favored either offense or defense. For instance, at the end of the nineteenth century, due to rapid advance in firepower (mostly in terms of range, speed and precision), a widespread belief circulated in European military circles that offense would be easy, and probably conducive to a swift victory\textsuperscript{16}. In more general terms, Karen Ruth Adams finds a statistical correlation between what she calls “offense dominant eras” and the frequency of wars\textsuperscript{17}. In a word, the international system is more prone to peace and stability when technology clearly makes it possible to: 1) draw a distinction between offensive and defensive weapons; 2) assess the relative superiority of offense over defense.

For practical purposes, the major issue with ODB theory is how to measure this balance. In the most concise statement, Charles Glaser defines it as “the ratio of the cost of the offensive forces the attacker requires to take territory to the cost of forces the defender has deployed”\textsuperscript{18}. The measurement issue is probably the most controversial element of the theory\textsuperscript{19}, as a number of problems need to be solved: how can we foresee the costs of both offense and defense before they actually take place? How can we do it, considering that these costs vary according to the nature and dimension of the territory to conquer? Are the costs of conquest enough, or should we also include the costs of keeping control over the seized territory in the offense component?


\textsuperscript{16} A number of accounts are available in S. MILLER, S. LYNN-JONES, S. VAN EVERA (eds.), Military Strategy and the Origins of the First World War, Princeton, NJ, Princeton University Press, 1991. The main problem with this view was that it focused just on the tactical dimension, thus failing to take into account the strategic advantage of defense. A. LOCATELLI, Tecnologia militare e guerra..., cit., pp. 70-74.

\textsuperscript{17} K. ADAMS, Attack and Conquer?..., cit.

\textsuperscript{18} C. GLASER, Rational Theory of International Politics..., cit., p. 43.

These and other problems have generated a lengthy debate, which is not possible to discuss here\(^20\). For our purposes, the main tenet of ODB theory is still worth investigation: whenever defense is (or is held to be) more expensive relative to offense, states will have an incentive to use force. This argument, _mutatis mutandis_, can be tested in the cyber-domain.

**The Offense/Defense Balance in Cyberspace**

The first problem when it comes to assessing the ODB in cyberspace is to define the meaning of cyberspace and cyber-attack. Given the complexity and pervasiveness of ICTs, it should surprise no one that different authors came up with different visions. For our purposes, suffice it to say that cyberspace includes both a physical and a virtual dimension. According to Derek Reveron, for example, “like the physical environment, the cyber-environment is all-encompassing. It includes physical hardware […]; information […]; the cognitive […]; and the virtual. When aggregated, what we think of as cyberspace serves as a fifth dimension where people can exist through alternate persona on blogs, social networking sites and virtual reality games”\(^21\). In the same volume, Brandon Valeriano and Ryan Maness write that “cyberspace is physical; that is, it has defined boundaries of main-frames, wires, hard drives and networks”, but, they also add: “it is important to know that the cyber world is restricted to the domains of human thought”; finally, they conclude, “perhaps the most important distinction of cyberspace is between the physical layer and the syntactic layer\(^22\). The dual nature of cyberspace (hard and soft, or real and virtual) makes of it a peculiar battleground, where actions can have different purposes, like destroying physical infrastructures (unlikely), or disrupting processes (quite likely). Secondly, and equally peculiar, is the centrality of Internet for both military and


non-military actors. While differences exist between civilian and military networks, they mostly use the same hardware and software. The result is two-fold: on the one hand, cyber-threats can take the form of either criminal activities or acts of war just depending on the target of the attack23 (see Figure 1). On the other hand, the sources of these threats vary conspicuously, ranging from hackers, to terrorists, to intelligence services. Similarly to the terrorist challenge, then, the definition of cyber-threats in terms of war poses a significant problem24. Fortunately, a narrow definition of cyber-attack serves our purpose nicely. Since our goal is to assess the ODB in cyberspace, we just need to consider those actions perpetrated by and aimed at state actors. We can then stick to Hersh’s definition of cyber-war as the “penetration of foreign networks for the purpose of disrupting or dismantling other networks, and making them inoperable”25.

Figure 1 - Top 5 Activities for Malware Destination by Industry (virus rate per e-mail).

(Source: Symantec Intelligence Report, August 2013, p. 25.)

Borrowing the terms of ODB theory, then, drawing a distinction between offense and defense becomes somewhat less complicated. Equally important, it is easier to assess their relative costs, as the main purpose of action is not to control a territory but to

23 A concise list of cyber threats includes viruses, logic bombs, Trojan horses, worms, etc. Their consequences are hardly confined to the civilian or military domain only. Just as an example, when a virus attacks a commercial website, it can slow down the Internet, with consequences for both private actors and governments.


compromise/ensure the effectiveness of a system or network. As for
the traditional domains of war, it is probably impossible to measure
the ODB as if it were an equation. Nonetheless, some features of
cyberspace suggest that offense has a comparative advantage over
defense. This largely depends on the following considerations:

1. **Vulnerabilities are key.** What makes cyber-attacks possible is
the existence of vulnerabilities in the targeted system. Put it
differently, viruses, worms, netbots and threats of this kind can
only take place if they have access to their target through a
network and, most importantly, if they can exploit flaws in the
software. But it is technically impossible to rule out flaws in
software designs (see figure 1) and practically unfeasible to
disconnect computers from the network.

The centrality of defense vulnerabilities, and the need to exploit
them fully to make the attack successful leads to an unpleasant
consequence: an incentive to preemptive attack. In the words of US
National War College professor Richard Andres, “one of the most
noteworthy characteristics of cyber-defenses is that they change
rapidly. Practically speaking, the only way to maintain the ability
to penetrate an opponent’s cyber-defenses is to continually probe
and alter them […] however, these preemptive actions can have
unanticipated and sometimes catastrophic consequences.”

![Figure 2 - Total Vulnerabilities Discovered by Month](image_url)

*Source:* Symantec Intelligence Report, August 2013, p. 18.

2. Progress in offense is faster than defense. Differently from the other domains, cyberspace is not natural but is the result of technological evolution. As such, its features (and the ODB) are constantly evolving. In this sense, both defense and offense develop and improve, as witnessed by the constant upgrading of hardware and software (or, in a different perspective, by their rapid obsolescence). So far, however, improvements in defense have been succeeding at a slower pace than progress in offense\(^{27}\). The end result is aptly summarized by Martin Libicki: “Offense-defense curves at levels that characterize today’s cyberspace favor the offense. That is, another dollar’s worth of offense requires far more than another dollar’s worth of defense to restore prior levels of security”\(^{28}\).

3. Attribution is difficult. As the source of the attack can be thousands of miles away, and the main vector for the attack rests on a network, identifying who actually perpetrated the offence is usually a difficult task. Moreover, considering that it may take just a handful of people to plan and execute the attack, it is quite easy for governments to deny responsibility. An example can be found in the 2007 attack on Estonian web sites: in this case, a botnet (i.e. a network of hijacked computers) was used to flood the servers with massive simultaneous requests, thereby producing a denial-of-service attack. Since many of the requests were traced back to Russia, Estonian authorities conjectured direct involvement from the Kremlin. Although the argument is plausible\(^{29}\), as of today there is no evidence of that.

The difficulty in attribution does not directly affect the ODB. However, at least indirectly, it favors offense, since it nurtures the illusion that the attack can go unpunished. This problem also makes retaliation more difficult, since one of the main requirements for retaliating an attack is to know who should be the target of retaliation. The end result is that cyber-deterrence is more difficult than nuclear or even conventional deterrence, which in turn lowers the expected costs of the attack\(^{30}\).


\(^{28}\) M. LIBICKI, Cyberdeterrence and Cyberwar, Santa Monica, CA, RAND, 2009, p. 32.


\(^{30}\) M. LIBICKI, Cyberdeterrence and Cyberwar..., cit.
Conclusions

Cyberspace, as shown by the origins of the Internet with the ARPA project in the early 1960s, was originally created as a force multiplier. The way it developed, as well as the growing dependence of the armed forces on networks, gave rise to widespread speculations on the possibility of future cyber-wars. Such a scenario does not seem likely in the short term, but recent episodes – like operational attacks during the 2008 Russia-Georgia war, or most evidently STUXNET against Iran – lead to investigating the growing importance of cyberspace for military purposes.

In these pages we tried to borrow the main proposition from ODB theory – namely, that war is more likely when offense is less costly than defense – to discuss whether we can expect military cyber-operations to be more frequent in the future. A cursory look at the main features of cyberspace suggests that offense has an advantage over defense. Or better, the prospect of the attacker being successful against given targets is higher than the prospect of the defender thwarting the aggression. Following this logic, then, we should foresee a growing number of cyber-attacks, if not at the strategic level, at least at the operational level31.

31 These terms are borrowed from M. LIBICKI, Cyberdeterrence and Cyberwar..., cit., chapter 6.