

Douhetian Lessons Applied to Combat in Cyberspace

CAPTAIN LUIS CELLES, FAB
ANDRE GONÇALVES

The formulation of a problem is often more essential than its solution, which may be merely a matter of mathematical or experimental skill.

—Albert Einstein

Human history is marked by conflicts of interest that often result in armed warfare. Consequently, states must anticipate such a situation in order to preserve their best interests and, at times, to ensure their survival. Historically, countries that prepare themselves for the possibility of future conflict, especially in terms of technological readiness, tend to have an advantage over others. Currently, we live in an information age that features the *Internet* as the central axis of communication in our global society. Indeed, our dependence on that computer network makes us realize that combat will likely occur in cyberspace. Interestingly, in terms of readying ourselves for such future strife, we would do well to look to the past—specifically, to aviation concepts articulated by Italian general Giulio Douhet, a pioneer of airpower strategy, during the early twentieth century.

All too often, sovereign states go to war to settle their differences, using any means necessary—including both old and new technology—to achieve their goals. Take, for example, the airplane. Less than a decade after its invention, various nations began using it to improve their combat capabilities. Its entry into military service has completely changed the face of warfare. Today, we observe a similar revolution with the advent of the *Internet* and its inclusion in all aspects of our lives. Conflict in cyberspace has become a reality—one that the military cannot afford to ignore. But how can one define a course of action regarding something that never existed before in the history of civilization?

To answer that question, this article examines the first eight chapters of Douhet's *The Command of the Air*, written between 1921 and 1927.¹ In that book, Douhet offers his impressions of this novel craft and suggests how it should be used in combat. The analogy to cyber warfare is evident: a new technology in the early stages of its capabilities begins to evolve rapidly in both the civil and military arenas and becomes involved in national defense. The article briefly summarizes the contents of each chapter and relates Douhet's discussion to the present situation with cyberspace. (Note that the titles of the first eight chapters of the Brazilian edition of *The Command of the Air*, used here, correspond to the eight sections of chapter 1, "The New Form of War," book 1, "The Command of the Air," in the American edition.)²

Chapter 1, "The Technical Means of Warfare"

In chapter 1, General Douhet reflects on the aircraft's entry into military operations as a weapon. Here we find his first criticisms of the persistent idea of using aviation as an auxiliary force to the navy and army, especially in exploration and reconnaissance missions. Douhet points to the logic of creating an independent force that could develop the airplane's full potential as a weapon of war. He predicts that future conflicts will involve all segments of a nation and that the latter should pay special attention to the available technical means on which the military will

depend to wage war. Douhet ends the chapter by addressing the necessity of studying as precisely as possible the ability of this new type of equipment on the battlefield, compared to that of land and sea weapons. Similarly, we should explore and perfect our existing technical capacity to carry out such action (a cyber attack) to realize military objectives in the event of war.

The conflict in South Ossetia in 2008, involving Russia and Georgia, will likely be remembered as the first altercation between two sovereign states in which a cyber attack preceded the outbreak of hostilities.³ That is, conflict began in the virtual world before commencing in the real world. Thus, the projection of military power started on land and then moved to the sea, the air, outer space, and now to cyberspace—its fifth dimension of performance. As we try to understand the magnitude of this change and prepare for a possible struggle in this environment, we must also quantify our cyber capabilities and range.

Chapter 2, “The New Possibilities”

Douhet observes that prior to the advent of aviation, wars were restricted to the land/water surface of the earth, some of it more conducive to ease of movement and access than others. Naturally, defenses positioned themselves to protect accessible areas coveted by the enemy, who could reach the desired territory only by breaking those defensive lines and pushing them backwards. Conversely, the defender can protect his territory only by keeping the attacker out of a defensive line.

Such assaults, however, were directly felt only as far as the range of the weapons employed. Though fully involved in the conflict, nations distinguished between combatants and noncombatants, so for the latter, life did not change appreciably in periods of either peace or war. With the introduction of the aircraft, such assumptions ceased to exist because these platforms were not limited by predetermined paths on the ground or in the water. The effects of combat were no longer restricted to the front lines because aircraft could fly over the lines of defense to reach targets within enemy territory. By the same token, all of the defense we know today will become irrelevant in the cyber environment because it is based on protecting against a physical rather than virtual attack. The number of fighter aircraft or antiaircraft missile sites that defend our territory simply won't matter against a cyber attack. Even worse, such a strike could be directed not only at military institutions but also at any one of the five rings (leadership, key production, infrastructure, population, and fielded forces) described by John A. Warden III.⁴

For example, attackers can use cyberspace to steal data from public and private organizations, use citizens as unwitting tools to spread false information, damage or destroy infrastructure, disrupt basic supplies (e.g., electricity, water, and banking services), and implicate political figures in fake scandals through the theft of personal data contained in e-mail or mobile messages. Since it is virtually impossible to protect anyone from this type of threat, we clearly need an organization prepared and trained to act in defense of democratic institutions at all levels (federal, state, and city) in all three branches of government (legislative, executive, and judicial) and any private segment of society that supports national security.⁵ This organization must be capable of acting in a virtual environment against a wide variety of enemies supported by a number of sources (e.g., other states, political or religious groups, criminal enterprises, etc.).

Chapter 3, “The Upheaval”

In this part of the book, Douhet explains how the capabilities of weapons used in World War I favored defensive instead of offensive actions and how the nations involved almost went bankrupt due to the effort required to fight in such a static way. That is, an increase of firepower in the arms used implies a corresponding increase of range and rate of fire; therefore, even

though the attacker possesses a better weapon, he has to face a stronger defense supported by machine guns and artillery. Consequently, these kinds of attacks demanded more men, guns, and supplies, thereby straining a nation's resources. Douhet concludes that, after the conflict, this experience led some nations to give utmost importance to building barriers and fortifications even though the airplane could easily overcome these obstacles and reverse the situation, giving an attacker the advantage.

Brazil has created structures for the purpose of protecting and enabling the use of armed forces in the cyber environment. According to the new Cyber Defense Policy established by the Ministry of Defense, effective protection against cyber operations depends not only on the military segment but also on Brazilian society as a whole, including private and civilian institutions.⁶ Malicious activity on the Internet instigated by amateur hackers is now taking the form of attacks carried out by professionals to further the cause of various organizations. For example, the cyber spying campaign known as Red October, which began in 2007, sought to obtain sensitive information and access to secure networks in different countries of the world. At least three attacks were directed at Brazil's diplomatic and scientific institutions.⁷ The inability to identify the perpetrator of such an attack makes it difficult to determine the purpose of obtaining such data.

Chapter 4, "The Offensive Arm"

Here, Douhet points out the difficulty of adopting a defensive attitude toward air weapons since, unlike land and sea forces, aircraft can attack from any direction, regardless of geographical or man-made barriers. Such an attitude would lead to a dilution of defensive forces because of the necessity of creating a defensive circle rather than a customary line of defense. He explains the futility of these dispersed forces completely protecting against a mass employment of aircraft. The difference between the speed of defensive ground forces and that of attacking aircraft would prevent the former from assisting the targeted area. Douhet suggests that, unlike the practice in previous conflicts, it is now necessary to have more people defending a target than those attacking, thereby changing the ratio of resources allocated between defense and attack in favor of the latter. He concludes this chapter with one of his most famous axioms: that one can conquer the air only by preventing the enemy's air operations by taking offensive action against his assets while they are still on the ground—not by stationing defenses in one's territory and waiting for him to attack.

Cyberspace can be used for both defensive and offensive strategies. DCA 1-1, Brazilian Air Force Basic Doctrine, includes among its many air force actions cyber defense, designed to protect friendly communication systems and information technology for command and control, to cause damage to corresponding enemy systems, and to gather relevant information about the opponent's structures.⁸ Use of the virtual environment in a conflict is not limited to offensive strategies to obtain an initial advantage; rather, we must keep in mind that this works both ways and that we will have difficulty identifying enemy targets for retaliation. Since anonymity is the trump card in this type of combat, we must use it in our favor, especially in actions aimed to build databases of likely threats and verify the extent of the enemy's combat capability (either offensive and defensive) in cyberspace so we can gauge his strengths and weaknesses. Furthermore, in light of the rapid development of threats, their wide range of possibilities, and the prospect of extensive damage, we must gather such information continuously—not just during a state of conflict.

Chapter 5, “The Magnitude of Aerial Offensives”

Analyzed outside its historical context, this chapter proved one of the most controversial sections of the book. Here Douhet advocates the use of explosive weapons, both incendiary and chemical, not only on military targets but also on the civilian population in order to affect morale and thereby reduce public support for the conflict. He further notes that a military unit would have prepared itself to withstand an attack from enemy artillery but not one from aircraft flying deep into the territory and therefore would suffer from the direct impact of aerial ordnance.

Douhet also compares the firepower of the British fleet’s potent battleships to that of a generic airplane, asserting that a two-ton bomb load of explosives in each aircraft would equal the broadside of three battleships, one of which would cost the equivalent of 1,000 such airplanes. Finally, he argues that in a clash between the two platforms, the aircraft would have the full advantage of employing its weapons with impunity.

Assessing Douhet’s proposal for attacking civilians from hindsight, in light of our familiarity with every major conflict of the last century, we know that he was wrong to imagine that only airpower could affect the morale of civilians to the point of demanding that their leaders surrender unconditionally. In truth, an air campaign never managed to get to the point of undermining the national morale, but perhaps a virtual conflict may have more success in this type of mission and, if not weaken morale, significantly subvert the people’s will to fight the opponent.

In Brazil during 2010, one-third of commercial dealings between businesses and consumers took place over the Internet. Research conducted in the following year showed that 48 percent of Brazilians have access to the Internet but that only 20 percent use it for shopping, primarily because of their lack of trust in such transactions.⁹ Despite its capacity to host a high volume of business (probably because of its speed and convenience), the Internet still faces strong opposition from Brazilians in terms of trustworthiness and credibility as a tool for doing business. The country’s federal (and most state and municipal) income tax collections, however, depend exclusively on the use of existing programs on the Internet to download and send forms. Moreover, with regard to electronic trading operations, we have the third-largest stock exchange in the world by market value.¹⁰ The number of current accounts with Internet access has grown by an average of 18 percent per year between 2002 and 2011, and in 2012 25 percent of all banking transactions occurred on the Internet.¹¹

What we see here is a kind of paradox: a nation highly dependent on the Internet market yet one that does not consider it a reliable tool for such transactions. Now imagine the repercussions in this market if its systems were shaken by the mass theft of personal information, the cancellation of bank or market orders, or the disruption of access for a couple of hours or days. This situation probably would be aggravated by the legal difficulty of punishing the guilty party (even if it were identified—a rare occurrence), thus exposing users of the system not only to its fragility but also to the invulnerability of the perpetrators.¹² Although measuring the financial loss caused by such attacks is difficult and inconclusive at best, we can assume that the problem is serious—witness the fact that in 2012 Brazilian banks invested a substantial amount of money in information technology to counter electronic fraud.¹³

Chapter 6, “The Command of the Air”

Douhet then reinforces the central idea his book: in war, mastering the air means victory and losing such dominance means defeat. He argues that to overcome a nation’s defenses, one cannot accept a stopgap or partial solution in efforts to prepare for war since aviation will prove essential to dictating the course of battle. He makes clear that future war will take place on three battlefields (land, sea, and air) and that each one will require a specialized force to undertake

different operations for various environments although all should be coordinated to assure victory. Thus, one cannot use aviation merely as an auxiliary of the army and navy; rather, it must constitute a third force employed for gaining command of the air.

Establishing cyberspace supremacy or a cyberspace domain, however, presents difficulties because it is a virtual dimension spread all over the world. Nevertheless, new technologies offer new solutions to fulfill an old objective—victory. In 2008, for example, a communications company was able to redirect, for 18 minutes, about 15 percent of all Internet traffic worldwide through the country in which it was located. China Telecom, the company responsible, denied culpability, pointing out that most traffic passes through the United States. Regardless of intention, we must recognize the magnitude of this feat, which involved a tremendous amount of data that could have been stored for further analysis.¹⁴

Extrapolating from Douhet, we can say that the next conflicts will have a new front—the virtual environment—and that we should be able to secure our use of the Internet while denying it to the enemy. To do so, we must have a force adequately staffed and trained for this purpose—one that acts on its own with independent objectives and doctrine in cooperation with other forces but not subordinated to them. Then, if the need arises, should we act accordingly (as we did when the air force became a separate branch), or should we anticipate the problem?

Chapter 7, “The Extreme Consequences”

Douhet next formulates two corollaries to support his idea that a nation must conquer command of the air to assure victory. First, he emphasizes that the security of a nation and, consequently, its defense, depends upon being in a position to conquer command of the air during conflict. Second, he notes that all defensive efforts in wartime should have as their objective the attainment of means for defeating air dominance. Douhet reaffirms that to control this domain, one must destroy the enemy’s ability to fly and that only aircraft capable of hitting targets both inside enemy territory (on the land and in the water) and in the air can do so. Further, he insists that only a separate air force (focused on combat in the air) can conquer an enemy’s command of the air—a notion that ran counter to his own country’s concept of national defense.

Aware of the controversial nature of his position, Douhet reinforces his thesis that it is necessary to look at this unique tool with fresh eyes and try to move away from old concepts and truisms, recognizing a new era in the evolutionary curve of conflict and incorporating the aircraft into military planning. He emphasizes that the efficiency of troops (and thus the defense of the nation) demands that we anticipate changes in the character of war instead of adapting ourselves after they occur. Continuing, Douhet points out that this change does not imply the extinction of land and naval forces; instead, he asks only that the nation acknowledge the importance of employing an air force independently rather than relegating it to the sidelines in an auxiliary role.

Similarly, a force that fights for the advantage in cyberspace should not be subject to any of the existing military commands. Furthermore, we must consider legal issues since characterizing cyber attack as a crime differs from considering it a hostile act of war, a distinction that raises some important questions:

- Should we have two (or more) different branches protecting cyberspace?
- If so, what are the boundaries of their jurisdiction?
- What happens if a soldier perceives a crime or a policeman detects an act of war in cyberspace?
- For that matter, how can we differentiate between a crime and an act of war in cyberspace?
- In cyberspace should a soldier also be a policeman, a policeman also be a soldier, or do we need a different type of professional with very specific competencies?

- Is it better to have several branches, each with its own cyber force performing its own job and, if necessary, exchanging information? Or should we have a unique branch that centralizes all important operations while the branches already established use their assets for specific needs as auxiliary forces—similar to the way the intelligence community operates?

An example of this complexity occurred in 2010 when a Stuxnet computer worm attacked nuclear facilities in Iran, not only affecting the virtual network but also causing physical damage.¹⁵ Would such an action constitute a crime or a hostile act against that nation? If a similar event occurred in Brazil, who would be responsible for identifying the culprit and suggesting a proportional response? The Federal Police? The Department of Justice? The Department of Defense? In such a situation, the responsibility to prevent, combat, and advise should reside in a “Cyber Force” having the freedom to respond independently of the characterization of the act itself (as a crime, act of war, act of terrorism, political action, etc.) to defend the state. In the information age, we can no longer waste time deciding who is responsible; instead, we must determine how to manage the problem. Secondary measures such as diplomatic actions, public statements for internal and external audiences, convening a crisis cabinet, and so forth, will all prove insignificant if we cannot stop a threat that could occur and disappear in a matter of hours. Just as Douhet advocated a force that would dominate the air, so must we establish an independent Cyber Force prepared to fight and win in cyberspace.

To protect the nation and its institutions, such a force should include both military and civilian professionals; should be guided by policies of the National Police, especially in handling defense and intelligence operations; and maintain open channels of communication with the auxiliary cyber services of the security and defense communities. In sum, the force would have a hierarchical structure with centralized control and decentralized execution, governed by its own regulations and guided by specific doctrine in line with the goals of the state. The Cyber Force commander or director should have direct access to the president and, respecting the democratic principle of checks and balances, should be subject to the same controls applied to the military forces and intelligence community by the judicial and legislative branches.

Chapter 8, “Independent Air Force and Auxiliary Aviation”

For the first time, Douhet uses the term air force to designate a branch of the armed forces whose purpose is to gain air dominance. This new force, independently of the others, must be prepared to fight alone in pursuit of its own objectives but always seeking common ground (i.e., national defense) with the navy and army. He agrees that both of those branches require specific aircraft to support their missions (his concept of auxiliary aviation). Douhet concludes this chapter and the first part of the book by maintaining that the army and navy should use such aircraft to pursue their own goals and not look to the air force for this purpose because this new institution has the unprecedented role of dominating the air in wartime.

Just as the use of the air should not be exclusive to the air force, much less the military, so should the use of the Internet not be exclusively delegated to an independent Cyber Force. Internet advancements (both in military and civilian fields) in the areas of services, leisure, social networking, communications, and so forth, are undeniable and should not be subject to either censorship or limitation. Thus, all branches involved in defense and security should use cyberspace but always to carry out tasks and reach their goals more efficiently. Toward that end, their personnel should receive specialized training, as do army and navy aviators as well as personnel in other government agencies. Thus, each sector would possess specialized assets, but the responsibility for fighting at the strategic, operational, and tactical levels to attain cyber supremacy/superiority should remain with the specific force created for this purpose. Apportioning this responsibility among all of the branches would encourage each one to attend only to its own in-

terests, leaving no one responsible for the network as a whole. Such a structure would find itself at a great disadvantage against a force under unified command and precise objectives (maintaining the domain of cyberspace and denying it to the enemy), capable of concentrating all of its power on the vulnerabilities of a dispersed opponent.

Conclusion

It is easier to disintegrate an atom than a prejudice.

—Albert Einstein

This article has shown that conflict in the virtual world is already a reality and that we must prepare ourselves for such an eventuality. However, the paths to choose from are obscured by the darkness of ignorance since we have not witnessed (at least not ostensibly) a clash in cyberspace comparable to a conventional war that would allow us to analyze and formulate a doctrine based on lessons learned and apply it to our defense strategy. For that reason, this article extrapolated the concepts of an airpower theorist who experienced a similar problem with another technology in a different time. Like the concepts of many other theorists, Douhet's faced strong resistance, but his ideas about the use of a new tool, its role in dictating the course of war, and the importance of a separate force with specific goals seem relevant to our handling of the cyberspace environment.

As did Douhet, we are experiencing a change in the evolutionary curve of conflict. The strategies of fighting in cyberspace are not yet well defined, but this new dimension will be a part of all conflicts from now on and will completely change the way we think, plan, train, and act in combat. Trying to anticipate the problem, the article examined the guidance of someone who had experienced a similar period of doctrinal revolution. Perhaps the most important lesson to learn from Douhet is that we must start to think in terms of a separate force to fight in cyberspace because using only portions of today's organizations for such a task will prove inadequate for national defense, as was the case with airpower until a separate air force emerged. By creating an independent Cyber Force, we will go a long way toward preparing ourselves for the conflicts to come. However, if we continue to treat cyber power as a means of assisting other forces attain their goals rather than embrace a separate Cyber Force, we will only prepare ourselves to fight a conflict that has already occurred—and history reveals that those who choose this path start at a disadvantage. Is that what we want? □

Nota

1. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC: Office of Air Force History, 1983).
2. *Ibid.*, 3–33.
3. Capt Paulo Shakarian, "The 2008 Russian Cyber Campaign against Georgia," *Military Review* (November–December 2011): 63–68, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20111231_art013.pdf.
4. See John A. Warden III, *The Air Campaign: Planning for Combat* (Washington, DC: National Defense University Press, 1988), 145–46.
5. Fernando Valeika de Barros, "The Cyberwar Has Begun," *Observatório da Imprensa*, accessed 1 May, 2013, http://www.observatoriodaimprensa.com.br/news/view/_ed712_a_ciberguerra_ja_comecou.
6. Brazilian Ministry of Defence, MD 31-02-P, *Cyber Defense Policy*, 2012.
7. "Red October: A Brazilian Perspective on the Attacks," *DefesaNet*, accessed 2 May 2013, <http://www.defesenet.com.br/cyberwar/noticia/9450/Outubro-Vermelho—Uma-visao-brasileira-sobre-os-ataques>.
8. DCA 1-1, *Brazilian Air Force Basic Doctrine*, 2012.
9. Leonardo Antonioli, "Statistics, Data and Projections on the Internet in Brazil," *To Be Guarany*, accessed 29 April 2013, http://tobeguarany.com/internet_no_brasil.php.

10. "Timeline Bovespa," Portal IG, accessed 26 April 2013, http://extras.ig.com.br/infograficos/ibovespa/internet_no_brasil.php.

11. Fabio Barros, "Internet Banking Is the Preferred Channel of Brazilian Users," *Convergência Digital*, accessed 27 April 2013, <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?inford=30231&sid=5#.UZDNofKBIdV>.

12. Adenele Garcia Ram, "Virtual Crimes," *Âmbito Jurídico*, accessed 29 April 2013, http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529.

13. José Pedro Teixeira Fernandes, "Cyberwar as the New Dimension of XXI Century Conflicts," *SciELO Portugal*, accessed 29 April 2013, http://www.scielo.gpeari.mctes.pt/scielo.php?pid=S1645-91992012000100005&script=sci_arttext; and Toni Sciarretta, "Banks Lose Up to R\$ 3.1 Billion to Fraud and Spend R\$ 4 Billion Safely," *Folha de S. Paulo*, accessed 29 April 2013, <http://www1.folha.uol.com.br/mercado/1247436-bancos-perdem-ate-r-31-bi-com-fraudes-e-gastam-r-4-bi-com-seguranca.shtml>.

14. Altieres Rohr, "China 'Hijacked' Internet Traffic for 18 Minutes, Report Shows," *Globo*, accessed 29 April 2013, <http://g1.globo.com/tecnologia/noticia/2010/11/china-sequestrou-trafego-da-internet-por-18-minutos-mostra-relatorio.html>.

15. Carlos Alberto Teixeira, "Stuxnet Virus That Attacked Nuclear Plants in Iran Was Created in Partnership by U.S. and Israel," *Globo*, accessed 3 May 2013, <http://oglobo.globo.com/tecnologia/virus-stuxnet-que-atacou-usinas-nucleares-no-ira-foi-criado-em-parceria-por-eua-israel-2836696>.



CAPTAIN Luis Eduardo Pombo Celles Cordeiro, (FABRA) (MBA in Public Management-Air Force University – Rio de Janeiro and is a Distinguished Graduate on the class 13 A – SOC-Maxwell AFB) is responsible for the discipline of Military Force Employment at the Brazilian Air Force Squadron Officer College (EAOAR)-Rio de Janeiro. He is also responsible for prepare the curriculum of the course as well teaching Air Force Basic Doctrine. Prior to his current job he was the Personal Administration Officer at the 5/8 Squadron – Santa Maria AFB. He is a pilot with more them 3,400 flying hours in the T-25, AT-26, AT-27, C-98, U-42, H-50, H-1H and H-60L.



Professor André da Costa Gonçalves is graduated in Literature (Portuguese Literature) from the University of Rio Grande and with a Master of Education, Culture and Communication in the Urban Periphery UERJ. He is currently professor of Portuguese language, literature and text production and research methodology at the Portuguese the Air Force University. He has experience in the field of letters in Portuguese Language and in Research Methodology.