HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR (Cambridge University Press, 2012)

2012, New York, Cambridge University Press
ISBN: 978-1-107-01108-3 (hardback)
Price: $124.00
Total Pages: 321 Pages

Keywords: Armed Conflict, Computer Network Attacks, Military Technology

Reviewed by: Brandon M. Basso
Journal of High Technology
Suffolk University Law School

Cyber Warfare and the Laws of War

"Until 2002, the idea of a country being attacked through its computer networks as a coordinated act of war was considered remote and largely dismissed as panic-mongering"[1]

In earlier years, military strategy revolved around a state's army physically overpowering another state's army to win a battle. Yet, now states overpower each other by attacking the other's computer network. In *Cyber Warfare and the Laws of War*, Heatherr Dinniss explains how the laws of war have changed to accommodate battles between computer networks.[2] Dinniss illustrates the effectiveness and efficiency of computer network attacks and how such attacks are more useful than traditional artillery attacks. Further, she suggests that, if utilized properly, computer network attacks expose the extreme vulnerability of states that are dependent on critical infrastructure such as dams and electrical grids.

Although this book discusses detailed topics regarding the evolution of cyber warfare, Heather Dinniss is more than qualified to write about such topics. Dinniss is a postdoctoral research fellow at the International Law Centre of the Swedish National Defense College.

---

[1] *See* Heather H. Dinniss, *Cyber Warfare and the Laws of War* 239 (James Crawford & John Bell eds., 2012).
[2] *See* Dinniss, *supra* note 1, at 1.

Further, she taught at the London School of Economics and Political Science and the School of Oriental and African Studies, University of London. Dinniss' research focuses on the impact of modern warfare on Hague regulations and international humanitarian law. More specifically, Dinniss focuses on the regulations that control advanced weapons systems and computer network attacks in armed conflict.

This book is written in a way that tracks the evolution of armed conflict. More importantly, the book illustrates the evolution of the laws of armed conflict and how such laws accommodate warfare revolving around computers. Moreover, early in the book, Dinniss illustrates how external factors of war such as diplomatic meetings between world leaders, economic incentives of war, and political pressures are now obsolete because computer attacks nullify all such factors. Further, Dinniss explained that the old mentality behind war was to "achieve a strategic military objective where the opponent conformed to the attacker's will – the intention being to decide the matter by military force".[3] Additionally, the outcome of the battle influenced political, economic, and overall diplomatic relationships between states. But now, modern warfare makes it difficult to identify who launched a computer network attack and what the motivation was for attacking – it is a quicker and more secretive process. Thus, the aforementioned external factors do not have time to happen.

Dinniss analyzes the laws that have evolved to accommodate armed conflict in the internet age. Further, she explains how armed conflict is now applied to computer attacks, and how such attacks can also be labeled 'hostilities'. Chapter 1 establishes a theme of 'transition' from artillery warfare to computer network attacks. Moreover, chapter 1 discusses a change in societal trends consisting of globalization, network-centric warfare, and digitization. Chapter 2 explains how the traditional definition of armed force is no longer applicable, but rather applies

[3] *See* Dinniss, *supra* note 1, at 23.

to the characteristics of a computer network attack. Moreover, chapter 3 analyzes the evolving trends in warfare by illustrating the responses to 'armed attacks' in a digital age. More importantly, this chapter discusses the difficulty that victims of cyber-attacks have in identifying that a cyber-attack occurred, where it came from, and the appropriate steps in responding to such an attack.

Additionally, when a computer-network is attacked, it is difficult for the entity who was targeted to distinguish between a civilian and a combatant attacker. Therefore, chapter 5 illustrates the kind of characteristics that are associated with a computer-network combatant rather than a civilian just sitting at their computer. The idea behind this characterization is to differentiate between rogue actors who should not be granted immunity to an innocent civilian who worked at a computer where the attack passed through. For example, a cyber-attack is not issued from one computer, but rather is sent through multiple servers making it difficult to identify who the attacker is. Therefore, chapter 5 discusses the specific intellectual property markings that are associated with combatant attackers and not associated with civilians. Later, Chapter 6 explains how computer network attacks are now incorporated into military strategy. However, Dinniss explains that a computer-network attack used for military strategy must meet the standards of a legitimate military objective and must be justified before being launched.

As with any laws of armed conflict, there are designated items that are immune from the destruction that accompanies armed conflict. Thus, chapter 7 focuses on the Hague Convention, which is the first international treaty, signed to protect certain property in the event of armed conflict. This chapter describes how digital works such as digital photographs, electronic documents and archives, and recordings etc. are all 'cultural property' immune from computer network attacks. Further, the chapter discusses how international humanitarian law has also

evolved to accommodate the protection of digital property in armed conflict. Lastly, chapter 8 informs the reader about the laws of weaponry during an armed conflict. Additionally, this chapter mentions article 22 of the Hague Regulations, and how weapons may be used to injure the enemy, but the use of such weapons must be limited to reach a military objective. However, Dinniss mentions that the regulations will have to change to accommodate computer network attacks because such attacks are now considered forms of weaponry. Further, Dinniss explains that computer network attacks will "require additional consideration as to their interpretation in the modern battlespace"[4]

Ultimately, Dinniss portrays the difficulty in amending an already existing set of international regulations and laws to accommodate a digital world of armed conflict. Dinniss illustrates the difficult dynamic of how computer networks attacks are forcing the reconstruction of already existing Hague regulations and humanitarian laws. Moreover, Dinniss most likely wrote this book for Court-Marshall attorneys who are well versed on Hague regulations and the limitations of weaponry in armed conflict. Further, this book would also benefit attorneys with a focus on international law, and also graduate-level scholars focused on foreign diplomacy. Overall, this book was similar to an 'Examples and Explanations' law book in that the writing was concise and to the point. For such a difficult topic to explain, Dinniss simplifies the ideas by using real life examples of (for example) a 12 year old boy who hacked the control network of a large Dam, or a military mission that found laptops of Al Queda members with plans of hacking a country's electrical grid, etc.

With that, I like how Dinniss incorporates real life terrorist activity to explain the increased use of computers in warfare. Additionally, Dinniss illustrates the U.S. government's

---

[4] *See* Dinniss, *supra* note 1, at 252.

underestimation of computer network attacks from terrorist. On the other hand, Dinniss explains that military adoption of high technology equipment used to combat such attacks has enhanced the military's capability to inflict force faster and more efficiently with fewer casualties.

To conclude, many people would benefit from reading this book because cyber security is a growing trend that people will read increasingly about in the news. Moreover, it is likely that there will be more computer network attacks than artillery attacks in the future, and the general public would benefit to know the characteristics behind such attacks before they occur. Military contingency operations have confiscated terrorist laptops that showed multiple visits to sites with sabotage, software, and 'cracking' information. Additionally, other terrorist laptops had engineering software codes and architectural models of dams to possibly issue a cyber-attack against the dam's network to stop functionality. However, if Dinniss used these examples in her book then it is likely that intelligence officials are well informed on these matters and are well prepared to combat any expected cyber-attacks. Ultimately, I encourage other students and lawyers to read Dinniss' book because it is very informative and provides detailed foresight on the incorporation of computer network attacks in military strategy.