CYBERSPACE
AND THE
USE OF FORCE

WALTER GARY SHARP, SR.

Aegis Research Corporation
cyberspace and the use of force

walter gary sharp, sr.

aegis research corporation
NOTE FROM THE AUTHOR

The opinions and conclusions expressed herein are those of the author and do not necessarily reflect the views of any governmental agency or private enterprise. This research is intended to provide as complete and useful an exploration as possible in the use of force in CyberSpace. This text is not intended, however, to substitute for the advice of legal counsel. Legal advice should only be sought from an attorney who can apply all relevant legal principles with a complete working knowledge of all of the relevant facts, purposes, and desires. Accordingly, the publisher and author make no warranty or representation, express or implied, as to the completeness, correctness, or utility of the information in this publication – and they assume no liability of any kind whatsoever resulting from actions based upon the contents of this book.
Dedicated to my parents,
Walter Harry Sharp, Jr.
and
Doris Mae Sharp,
who taught me to value peace and have faith in the law.

Published February 1999.
Printed in the United States of America.
### Table of Contents

Preface ........................................................................................................ ix  
Acknowledgements ..................................................................................... xi  
About the Author and Publisher ............................................................... xiii  
Executive Summary ..................................................................................... xiv  

**Part I: Introduction**

- **Chapter 1** Applying International Law in Cyberspace ...... 1  
- **Chapter 2** Military Applications of Cyberspace .......... 15  

**Part II: The Law of Conflict Management – The Legacy of War**

- **Chapter 3** The U.N. and Contemporary *jus ad bellum* ...... 27  
  - Evolution of *jus ad bellum* ........................................ 27  
  - Contemporary *jus ad bellum* ................................. 33  
  - Self-defense and the use of force by states ........... 37  
    - Necessity and proportionality ........................... 37  
    - Collateral damage and injury to civilians ....... 40  
    - Anticipatory self-defense ............................... 43  
    - Articles 2(4) and 51: Closing the gap .............. 44  
  - Security Council authority to use force ....... 49  
  - Conclusion ........................................................... 52  

- **Chapter 4** The Common Article 2 Threshold ............... 55  
  - Evolution and significance of the threshold ........ 55  
  - Defining an armed attack .................................. 58  
  - Conclusion ......................................................... 67  

- **Chapter 5** Delineating the Rules ............................... 71  
  - Sources of international law ............................ 71  
  - Reliance upon state practice ........................... 73  
  - Conclusion ........................................................... 77
Part III: State Activities in CyberSpace –
Defining What is a Use of Force and an Armed Attack

Chapter 6
Application of Existing Rules ...................... 81
Introduction ................................................. 81
Obligation to settle by peaceful means .......... 83
Political and economic force ....................... 88
Threats of the use of force .......................... 93
Violations of international law ................... 97
Unarmed, non-military physical force .......... 101
Protection of nationals abroad .................. 104
Indirect armed force ................................ 110
Armed attack ............................................. 113
Conclusion .................................................. 118

Chapter 7
Selected Issues – Computer Espionage and
Computer Network Attack ....................... 123
Introduction ................................................ 123
Computer espionage ................................. 123
Computer network attack ....................... 132
Conclusion .................................................. 134

Part IV: Conclusion

Chapter 8
Core Principles and Final Reflections .......... 135

Abbreviations .............................................. 144
Glossary .................................................... 145
Document Annex ........................................ 157
Index ........................................................ 233
LIST OF FIGURES AND TABLES

Figure 1  The Charter *jus ad bellum* Paradigm ............ 53  
Figure 2  The Application of International Law .......... 68  
Figure 3  The Rules Defining the Use of Force .......... 78  
Figure 4  Use of Force Analysis ............................. 120  

Table 1  Use of Force Principles ............................... 143

TABLE OF CONTENTS FOR DOCUMENT ANNEX

<table>
<thead>
<tr>
<th>Document</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A  Charter of the United Nations (excerpts)</td>
<td>159</td>
</tr>
</tbody>
</table>
| B  General Assembly Resolution 53/70 (1998),  
   *Developments in the field of information and telecommunications* | 185  |
| C  U.S. *Explanation of Vote* for G.A. Res. 53/70                      | 189  |
| D  Hague Declaration (IV, 1) of 1899                                     | 191  |
| E  Hague Declaration (XIV) of 1907                                      | 193  |
| F  Critical Infrastructure Protection:  
   A New Era of National Security                                      | 195  |
| G  General Assembly Resolution 3314 (1974)  
   *Definition of Aggression*                                           | 211  |
| H  Enclosure A, Standing Rules of Engagement  
   for US Forces                                                        | 219  |
PREFACE

The lawfulness of the use of force by states against one another is one of the most challenging, contentious, and important issues in international law. With the advent of computers and the Internet, technology has made this issue even more elusive and complex. Issues that involve the use of force in CyberSpace, however, can be, and should be, initially viewed simply as an application of existing international law. Only until the international community fully understands the application of existing international law, and therefore the gaps that may exist in that law, should it move forward with attempts to further regulate activities in CyberSpace.

At any given time during the growth of a new technology, the law – particularly international law – is rarely comprehensive. Legal advisers must apply existing law to the new technology. When treaty law fails to look prospectively, state practice slowly defines the boundaries of what is lawful. This book specifically examines which peacetime state activities in CyberSpace constitute an unlawful threat or use of force and when states have the right to use force in self-defense in response to an unlawful threat or use of force that constitutes an armed attack.

This analysis applies the existing international law paradigm that governs the use of force to rapidly advancing technologies which permit states to manipulate computers and computer dependent systems in ways that were not foreseen ten years ago. It is hoped that this will serve as a useful introduction and a starting point for the analysis of all use of force issues under international law, and specifically, all use of force issues that arise in CyberSpace. Although this book is intended to be a comprehensive overview of all use of force issues, any such attempt in such a short text will undoubtedly omit countless
possible references, supporting arguments, counter arguments, and
nuances that could have been made in a longer treatise. Where I
believe the law is settled, I make the point concisely and move on.
Where there is disagreement among jurists, I provide a summary of
the major views, and then explain what I believe to be the better
approach and why.

The issue of when a state may lawfully use force against
another state is very important, and warrants a thorough discussion
in isolation. Accordingly, this book only analyzes in detail the use
of force by a state against another state or states without Security
Council Chapter VII authority. Although explained very briefly in
Chapter 1, this book does not address in any detail the use of force
by a state against terrorists, organized criminals, and other nonstate
actors; the broader issue of how the peacetime regime of
international law, other than the law of conflict management, may
restrict state activities in CyberSpace; the application of the law of
armed conflict to the use of force in CyberSpace once hostilities
have commenced; the effect of United States domestic and foreign
law on state activities in CyberSpace; or the effect of Security
Council Chapter VII authorization on the lawfulness of state
activities in CyberSpace.

Though referenced in detail for lawyers, this text provides
the legal background to make it a useful desk reference for
government officials, military operators, students, and others who
are interested in the application of international law in CyberSpace.
The first five chapters will provide the legal and factual foundation
necessary to a full understanding of the core analysis of the book
found in Chapters 6 and 7. The final chapter will extract from
previous discussions of the entire book those guiding principles
that form the basis for analyzing all use of force issues.

WALTER GARY SHARP, SR.

Falls Church, Virginia
23 February 1999
ACKNOWLEDGEMENTS

This work is based upon six years of research and experience in the legal arena of national security law and information operations – and to my good fortune, exposure to some of the finest lawyers, military commanders, operators, government officials, and scholars who have added their insights and contributions to my thinking over the years. To the extent that this book is helpful, I owe a special debt of gratitude, albeit anonymously, to everyone that I have had the pleasure of working with over the years who have collectively helped shape my views on national security law, deterrence, and the use of force in CyberSpace. To the extent that this book fails to fulfil your expectations, I accept full responsibility.

Of particular note, I would like to thank the following colleagues at Aegis Research Corporation for their insightful review and superb suggestions from an operator’s view that tremendously helped shape the usefulness and readability of the final product: William H. Geiger, Robert M. Huffstutler, Donald L. Hardison, Richard P. Moore, Scott D. Billigmeier, Joyce M. Weymouth, Jerome M. Wucher, and Bonni Thompson. I owe a special thanks to Thomas C. Wingfield, Esquire, for his superb editorial assistance and substantive review, as well as his assistance in assembling the document annex.

The editorial assistance of my loving wife, Anne, who meticulously read a number of drafts countless times, was also invaluable. Without her daily support, this book would not have been finished on schedule.

I also owe a special thanks to Captain William Gravell, U.S. Navy. While serving on the Joint Staff during the formative years of information operations, Captain Gravell did more than any
other person in the U.S. Government to help identify the problem of information vulnerabilities in the age of the Internet and to help shape a national response thereto. His substantive review of this text from a warfighter’s perspective was invaluable.

Finally and most importantly, a very special thanks goes to William H. Geiger, President and CEO of Aegis Research Corporation, who commissioned the work of this book as a small part of his dedication to and respect for the rule of law in national security affairs.

Appreciation is also gratefully acknowledged to the following organizations that either posted or provided electronic versions of four of the documents provided in the Document Annex of this book:

The Fletcher School of Law and Diplomacy of Tufts University for an electronic copy of the Charter of the United Nations found in Document A.

The International Committee of the Red Cross for electronic copies of the 1899 Hague Declaration (IV,1) found in Document D and the 1907 Hague Declaration (XIV) found in Document E.

The United States Army Judge Advocate General’s School for an electronic copy of Enclosure A to the Standing Rules of Engagement for US Forces found in Document H.
ABOUT THE AUTHOR AND PUBLISHER

WALTER GARY SHARP, SR., is a principal defense and national security policy analyst at Aegis Research Corporation, and an adjunct Professor of Law at Georgetown University where he teaches graduate seminars on International Peace and Security and United Nations Peace Operations. Author of a text on United Nations Peace Operations and numerous other journal articles and papers on international law, deterrence, and the rule of law, he holds a Master of Laws (International and Comparative) from Georgetown University Law Center, a Master of Laws (Military Law) from The Judge Advocate General’s School, a Juris Doctor from Texas Tech University School of Law, and a Bachelor of Science (Aerospace Engineering) from the U.S. Naval Academy. Professor Sharp is a retired Marine judge advocate who previously served as Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff.

AEGIS RESEARCH CORPORATION is a leading provider of world class expertise in information operations (policy, strategy, and analysis), information security, threat analysis, threat characterization and countermeasures, mission planning and simulation, security implementation support, comprehensive enterprise strategy development, enterprise protection planning, and professional technical services for the federal national security community, state and local governments, and U.S. corporations.
EXECUTIVE SUMMARY

Information technology is redefining national security and how states use force. At the same time that it empowers states and their commercial infrastructures, information technology makes them more accessible and vulnerable to attack in CyberSpace. The anonymity afforded by information technology undermines deterrence and limits a state’s ability to use force in self-defense. Maintaining a credible ability to use force in CyberSpace is, however, lawful and a fundamentally important aspect of deterrence and the maintenance of international peace and security.

International and national law governs, but does not prohibit per se, state activities that involve coercion and the use of force in CyberSpace. States have an international obligation to act in good faith in settling their disputes by peaceful means and to refrain from the threat or use of force against the territorial integrity or political independence of another state. States, however, never lose their right to use necessary and proportional force in self-defense – although that right may not always justify an armed response.

What constitutes a prohibited ‘threat or use of force’ in CyberSpace is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances. Computer espionage, computer network attacks, and threats to use force, as well as political, economic, non-military, and indirect armed force, may all constitute a use of force in CyberSpace. Although a use of force does not always rise to the scope, duration, and intensity threshold of an armed conflict that invokes a state’s right of self-defense, international law clearly permits a state to respond in self-defense when attacked through CyberSpace. The United States has the right under existing international law to respond with military force, for example, if a state destroyed or significantly damaged the New York Stock Exchange by the use of computer viruses or other offensive cyber-tools.

The best way to accurately predict what may be considered a use of force or an armed attack under international law is by studying state practice. This text provides a detailed analysis of existing international law and state practice that reveals which state activities in CyberSpace may constitute a use of force and an armed attack that invokes a state’s right to use force in self-defense.
CYBERSPACE AND THE USE OF FORCE

Developments in telecommunications and information in the context of international security

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the security of States, …

United Nations General Assembly
December 4, 1998

Part I: Introduction

Chapter 1: Applying International Law in CyberSpace

When new technology provides one state a potential military advantage over another, the disadvantaged will quickly seek to outlaw or regulate those military applications that may be used as a new means or method of warfare, i.e., a use of force between states. When the military potential of hot air balloons frightened the international community, for example, an attempt was made to outlaw aerial bombardment. At the First Hague Peace

---

Conference,\textsuperscript{2} the Russians proposed a prohibition on “the discharge of any kind of projectile or explosive from balloons or by similar means.”\textsuperscript{3} This proposal resulted in an international norm signed and ratified by 25 states that prohibited “for a term of five years, the launching of projectiles and explosives from balloons, or by other new methods of a similar nature.”\textsuperscript{4}

This norm was reaffirmed during the Second Hague Peace Conference in 1907, when 27 states signed a similar declaration that was also intended to be limited in time.\textsuperscript{5} Although the initial reaction was to outlaw the activity, the perceived advantages of aerial bombardment caused a more reserved attitude within the international community as aerial navigation advanced.\textsuperscript{6}

\textsuperscript{2} The First Hague Peace Conference was held in 1899. It was the first major international effort to regulate the means and methods of warfare since codification of international law first began in 1856. DOCUMENTS ON THE LAWS OF WAR 2-3 (Adam Roberts & Richard Guelff eds., 2d ed. 1989).

\textsuperscript{3} THE LAWS OF ARMED CONFLICTS 201 (Dietrich Schindler & Jiri Toman eds., 3d ed. 1988).

\textsuperscript{4} Declaration (IV, 1) to Prohibit for the Term of Five Years the Launching of Projectiles and Explosives from Balloons, and other new Methods of a Similar Nature, Jul. 29, 1899, \textit{reprinted in} THE LAWS OF ARMED CONFLICTS, \textit{supra} note 3, at 201, 202-05. Declaration (IV,1) is provided as Document D of the Document Annex.

\textsuperscript{5} Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons, Oct. 18, 1907, \textit{reprinted in} THE LAWS OF ARMED CONFLICTS, \textit{supra} note 3, at 201, 206. This declaration was subsequently ratified by 20 states, but was only intended to remain in force until the Third Hague Peace Conference. There was never a third conference, and the declaration is still formally in force. Both the United States and Great Britain ratified this declaration. \textit{Id.} at 201, 206. Declaration (XIV) is provided as Document E of the Document Annex.

\textsuperscript{6} See THE LAWS OF ARMED CONFLICTS, \textit{supra} note 3, at 201.
attempts in 1907 to prohibit aerial bombardment permanently resulted only in the insertion of the language “by whatever means” to Article 25 of the Hague Regulations on land warfare which prohibits the attack or bombardment of undefended towns and villages.7

As silly as this historical example may now seem in hindsight after a century during which aircraft have played such a critical role in warfare,8 it demonstrates two approaches of trying to restrain the feared but undemonstrated military potential of advancing technology. At first, the international community attempted to establish an outright prohibition on aerial bombardment. Although some would describe this form of prohibition as arms control, it was actually an attempt to make aerial bombardment an unlawful method of warfare under the law of armed conflict. When an outright prohibition failed to gain consensus, the international community resorted to regulating the military potential by restricting how the technology could be used under the law of armed conflict.

Despite the initial reaction of the international community to prohibit outright aerial bombardment, the end result of the First and Second Hague Peace Conferences was simply an application of existing international law to new technology. Both of these

---

7 Id. at 201.

8 For a more contemporary example, consider the initial outcry of the international community to outlaw horrific environmental damage like that which occurred during the Persian Gulf War. When the debate settled, the international community accepted that an absolute prohibition on environmental damage during armed conflict was unworkable, that such destruction was already prohibited by the laws of armed conflict, and that additional proscriptions were not necessary. See, e.g., Walter Gary Sharp, Sr., The Effective Deterrence of Environmental Damage During Armed Conflict: A Case Analysis of the Persian Gulf War, 137 MIL. L. REV. 1 (1992).
Part I: Introduction

Hague Conferences attempted to utilize the law of armed conflict as a way to prohibit or regulate the activity, and presumed the activity in question was a use of force. In 1923, a commission of international jurists completed the Hague Rules of Air Warfare. Although these rules were never adopted in any legally binding form, they were an application of the customary norms and general principles of the law of armed conflict to the use of aircraft in war.

Only when the military applications of new technology are truly abhorrent and unacceptable under all circumstances, such as chemical and biological warfare, can the international community gain the consensus to prohibit those applications as means or methods of warfare. When the consequences of new technologies, however, fall beyond the defined parameters of acceptable activity, as was the case with aerial bombardment, the new means and methods of warfare are simply regulated by existing law, and when necessary, treaty law and evolving state

---


10 The Laws of Armed Conflicts, supra note 3, at 207. For a detailed and excellent discussion of the application of international law to the use of aircraft during armed conflict that is widely used within the Department of Defense as the definitive reference on the law of air warfare, see W. Hays Parks, Air War and the Law of War, 32 A.F. L. Rev. 1, 1-225 (1990).

practice. We should not rush to conclude that applications of new technology to military purposes should be prohibited outright or that they are not implicitly regulated by existing international law.

The prospect of hostile state activities and military operations in CyberSpace has elicited a pattern of concern in the international community reminiscent of the balloon warfare experience. When the legal community first considered the legal regime that governed state activities and military operations in CyberSpace, some U.S. government attorneys stated rather boldly that the application of modern information systems technology to military purposes was so new that no law applied. **It now seems almost universally accepted that a considerable body of international law does indeed apply to the use of force by states in CyberSpace.**

In parallel to the initial reaction of the international community to the military potential of hot air balloons, the epigraph to this book on page one reflects the international community’s concern over the potential for damage and disruption caused by military operations against and through information systems linked by the Internet. It is excerpted from a United Nations General Assembly resolution that resulted from an initiative of the Russian Federation. This resolution calls upon Member States to promote multilateral “consideration of existing and potential threats in the field of information security” and invites them to inform the Secretary-General of their views on several detailed issues relating to information security.¹² Although couched in terms of criminal and terrorist threats, *i.e.*, the use of force by non-state actors, it was initiated in the First Committee

---

Part I: Introduction

which concerns itself with disarmament.13 The unavoidable momentum of the international community in the First Committee will likely yield an attempt to prohibit certain military applications of the Internet, i.e., the use of force by states in CyberSpace. The likely result, however, will not be new international norms that substantially outlaw state activities in CyberSpace, but rather a debate, and perhaps a partial consensus, on the application of international law to the use of force by states in CyberSpace.

For the purpose of analyzing what constitutes a use of force or an armed attack, there are three relevant categories of international law. First, the peacetime regime of international law

---

13 This point was also implied in the United States Explanation of Vote after it joined in the adoption of G.A.Res. 53/70 by consensus. The United States explained:

The General Assembly’s adoption of the resolution in plenary will launch the international community on a complex enterprise encompassing many interrelated factors which delegates to the First Committee do not ordinarily address. For example, the topic includes technical aspects that relate to global communications – as well as non-technical issues associated with economic cooperation and trade, intellectual property rights, law enforcement, anti-terrorist cooperation, and other issues that are considered in the Second or Sixth Committee.

The United States Explanation of Vote is provided as Document C of the Document Annex. The General Assembly distributes most of its agenda items to one of seven main committees: the First Committee, which considers disarmament and related security issues; the Special Political Committee, which discusses political questions not dealt with by the First Committee; the Second Committee, which considers economic and financial matters; the Third Committee, which considers social, humanitarian, and cultural questions; the Fourth Committee, which is responsible for decolonization issues; the Fifth Committee, which considers administrative and budgetary matters; and, the Sixth Committee, which considers legal issues. U.N. DEPARTMENT OF PUBLIC INFORMATION, EVERYONE’S UNITED NATIONS: A HANDBOOK ON THE WORK OF THE UNITED NATIONS 15-16 (1986), U.N. Sales No. E.85.I.16.
Chapter 1: Applying International Law in CyberSpace

governs the conduct of states during peacetime, and it remains in place during armed conflict to the extent it is not inconsistent with a state of hostilities. While treaties requiring certain levels of trade between two states will be terminated when those two states become engaged in armed conflict, for example, peacetime environmental treaties will continue to impact a naval commander’s decision to sink an oil tanker running a blockade during armed conflict. Second, the law of conflict management is a part of the peacetime regime of international law that defines and governs the use of force between states during peacetime. It is a part of the peacetime regime that remains in place during armed conflict. Before armed conflict, the law of conflict management governs the use of force between states, and during armed conflict the law of conflict management principally imposes an obligation on states to terminate the hostilities as soon as possible consistent with their own self-defense requirements. Under the law of conflict management, a use of force that reaches a certain scope, duration, and intensity will establish an armed conflict as a matter of law. Third, the law of armed conflict governs the actual conduct of hostilities. This body of law specifically authorizes a wide range of force during armed conflict that is otherwise unlawful during peacetime.

Although a considerable body of international law applies to the use of force by states in CyberSpace, its application is not always obvious and many questions remain surrounding precisely how international law relates to the use of force in CyberSpace. For example, what constitutes a use of force in CyberSpace? When are states allowed to use force against each other in CyberSpace? How does international law prohibit or govern the use of force and other state activities in CyberSpace? Does international law impose any restrictions on state activities in CyberSpace that are not considered a use of force? What constitutes an armed attack in CyberSpace? When does an armed conflict exist between two or more states? Can state activities in
Part I: Introduction

CyberSpace cause an armed conflict? When does a state have the right to use force in self-defense? Is computer espionage lawful? Are computer network attacks lawful? Do computer network attacks constitute a use of force? When can a state use force to defend itself against computer network attacks? These, and many other important questions, will be answered in Chapters 6 and 7 of this book.

There are a number of important issues, however, that will not be addressed in this book because it is intended to analyze only use of force issues between states under the international law of conflict management. This book, for example, will not discuss the use of force by a state against recreational hackers, terrorists, organized criminals, and other nonstate actors. The use of force by a state against these nonstate actors is a law enforcement issue that must be principally addressed through cooperative bilateral and multilateral extradition and mutual legal assistance treaties.

Despite that a nonstate actor can cause identical damage to a state’s information infrastructure as can a state actor, a hostile, transnational activity in CyberSpace committed by a nonstate actor remains a law enforcement issue. The issue of state and nonstate sponsorship, however, may be very factually complicated by a number of circumstances, such as the activities of state-owned commercial enterprises and surrogate actors, as well as the anonymity afforded by technology. Nevertheless, the legal analysis remains rather straightforward. Determining when state-owned commercial enterprises, for example, are acting as a commercial enterprise or at the direction of a state is a determination surrounding facts, such as who controls the enterprise, who directs the activity, and the nature of the activity itself. It is not an issue of law.

Consequently, from a legal perspective, all hostile, transnational activities in CyberSpace are either nonstate-sponsored and thus a crime addressed by national and peacetime treaty law, or they are state-sponsored and thus a use of force governed by the law of conflict management and the law of armed conflict. Notwithstanding what the destructive effect may be, hostile, transnational activities in CyberSpace committed by recreational trespassers, terrorists, criminals, and other nonstate actors do not constitute a use of force within the meaning of the law of conflict management. Even a hostile, destructive act by a military service member or other government employee is a
These treaties are a part of the peacetime regime of international law, but they are not a part of the law of conflict management.

This book will also not address the broader issue of how the peacetime regime of international law, other than the law of conflict management, may restrict state activities in CyberSpace. Depending upon the circumstances, there are many treaties, and international regulations that have the force of law, that may restrict or prohibit certain state activities in CyberSpace. These treaties include, for example, those that regulate the use of satellites, telecommunications, outer space, and the law of the sea.

Similarly, this book will not address the application of the law of armed conflict to the use of force by states in CyberSpace once hostilities have commenced. At a point along the spectrum of interstate activities called the line of belligerency, a use of force by a state establishes an international armed conflict as a matter of law and the law of armed conflict applies. Even though the law of conflict management continues to apply during armed conflict, the law of armed conflict specifically authorizes a state to use all necessary and proportional force not otherwise prohibited by the law enforcement issue if the act was conducted in his or her private capacity and not at the direction of a state. Similarly, the ineffectiveness of law enforcement arrangements among cooperative states to address the problem of hostile, transnational activity in CyberSpace by nonstate actors does not change a crime to a use of force or the basic nature of the legal issues.

The complete refusal or unwillingness of a state, however, to cooperate in the suppression or prevention of an acknowledged nonstate-sponsored hostile, transnational activity in CyberSpace that originates in its sovereign territory constitutes state-sponsorship of a use of force ipso facto – thereby invoking the law of conflict management which may authorize a use of force in self-defense against such a state or the nonstate actors in that state. In the absence of any state-sponsorship of terrorist or criminal activities, a use of force by a state against those nonstate actors in the sovereign territory of another state without that state’s consent may rise to the level of an unlawful use of force against that territorial state.
law of armed conflict that is required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources.

Furthermore, this book will not address the effect of United States domestic and foreign law on state activities in CyberSpace. Any number of state activities in CyberSpace that are lawful under international law may nevertheless be highly regulated or unlawful under the national law of one or more states. For example, if the military forces of one state are conducting activities in CyberSpace that originate in their own state and target another state, but are transmitted through the telecommunications infrastructures of five other states, the national laws of seven states may apply in addition to relevant international law. In the United States, activities that involve intelligence collection, espionage, the nonconsensual penetration of computers to determine the identity of an attacker, and the counterattack of hackers through servers and systems not belonging to the hackers, are highly regulated and under some circumstances, may be unlawful. The Internet is like a global party-line, and it can be very challenging under the domestic law of the United States for the law enforcement and intelligence communities to find the authority to monitor or intercept transmissions when U.S. citizens are online.

Finally, this book will not address the special circumstances of state activities that have been authorized by the United Nations Security Council under its Chapter VII coercive authority. Article 39 of the Charter of the United Nations empowers the Security Council to authorize the use of force to maintain international peace and security under international law at a threshold lower than when states are authorized to use force in self-defense. A blockade, for example, that would be otherwise unlawful under international law if committed by a state would be lawful if authorized by the Security Council under its Chapter VII authority. Similarly, most state activities in another state are
unlawful without the territorial state’s consent; however, state activities conducted during a United Nations peace operation in a state without the territorial state’s consent is lawful if authorized by the Security Council under its Chapter VII authority. Furthermore, Article 103 of the Charter preempts most international obligations of states if they conflict with their obligations under the Charter. Consequently, a state activity that otherwise may be deemed an unlawful use of force under international law may be lawful if authorized by the Security Council under its coercive Chapter VII authority.

The primary focus of this book, therefore, is to examine the two threshold issues of:

(1) which peacetime interstate activities in CyberSpace constitute a threat or use of force under the international law of conflict management, and

(2) when does such a threat or use of force constitute an armed attack under the international law of conflict management such that a right to use force in self-defense exists?

These threshold issues are two of the most important issues of the law of information conflict (LOIC), which is the composite of the peacetime regime of international law, the law of conflict management, and the law of armed conflict that regulates the conduct of all state activities in CyberSpace. It embodies the application of the entire peacetime regime as well as the entirety of the laws of conflict management and armed conflict to state activities in CyberSpace. A complete study of the law of information conflict that includes a discussion of the five areas not addressed by this book is reserved for subsequent discussions to allow for a very focused analysis in this book detailing the affect of the law of conflict management on the use of force between states in CyberSpace.
There are a number of other foundational questions, however, that should be addressed prior to the discussion of these two threshold issues. What is CyberSpace, for example? What is it about CyberSpace that makes states a vulnerable target? Why do states want to use force in CyberSpace? What is the law of conflict management? When do states have the right to use force? What responsibility does the Security Council have to use force? What is the line of belligerency? What is the law of armed conflict, and how does it help define what constitutes a use of force and an armed attack under the law of conflict management? These, and many other questions, will be answered in Chapters 2 through 5.

Chapter 2 is a factual foundation. It defines CyberSpace as the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web. It explains why CyberSpace makes a state vulnerable; it provides examples of how those vulnerabilities can be exploited; and it illustrates how CyberSpace is simply another medium or environment through which states can either use force or support the use of force. Finally, it concludes that states are very likely to develop military applications of CyberSpace.

Part II provides the legal foundation necessary to understand what constitutes a use of force or an armed attack in CyberSpace under international law. After a brief historical review of the evolution of the law of conflict management, Chapter 3 provides a detailed discussion of the contemporary norms under the Charter of the United Nations that regulates the use of force between states during peacetime. It details when states are authorized to use force under international law against another state as well as the responsibility of the United Nations Security Council to authorize the use of force against states to maintain
international peace and security. Chapter 3 also provides a detailed discussion of the principles of necessity, proportionality, unnecessary collateral damage or injury to civilians, and anticipatory self-defense.

Any meaningful legal foundation of the use of force between states must discuss the interrelationship of the law of conflict management with the law of armed conflict. Although the law of armed conflict regulates only the use of force during hostilities, Chapter 4 examines in depth the one provision within the law of armed conflict that is widely accepted as the threshold test for when armed conflict exists between states. The application of this provision by states is critical in determining what constitutes a use of force and an armed attack under the law of conflict management. The terms hostilities, armed conflict, and war are used throughout these discussions. While these terms are frequently used interchangeably, the term hostilities only generally refers to a state of enmity between states\(^{15}\) and it has no specific legal meaning under international law. It is used to generically refer to either armed conflict or war. As explained in more detail in Chapter 4, the terms armed conflict and war actually refer to the same state of hostilities between states, but war is determined as a matter of law and armed conflict is determined as a matter of fact. Chapter 5 closes the legal foundation provided in Part II by melding Chapters 3 and 4 to form the basic principles that support the analysis to follow in Part III.

The two chapters of Part III constitute the core analysis of this book. They detail what constitutes a use of force and an armed attack under international law. Chapter 6 analyzes and then relates the existing international norms that govern the use of force between states to the activities of states in CyberSpace. It dissects

\(^{15}\) Black’s Law Dictionary 665 (5th ed. 1979).
the obligations of states to settle their disputes by peaceful means and analyzes when political, economic, and non-military force can constitute an unlawful use of force and an armed attack. This chapter also determines when a threat to use force is unlawful and when violations of international law or the indirect use of force can constitute an unlawful use of force. The topic of threats to use force is very interesting because it moves beyond an analysis of the legal issues based upon objective facts into the realm of the intent of the acting state and the perceptions of a potential victim state, i.e., a discussion of hostile intent. It also details when states can lawfully use force to protect their nationals abroad. Chapter 6 concludes with a detailed discussion of what constitutes an armed attack under international law and a graphic summary of Chapters 3 through 6.

Chapter 7 then applies the rules discussed in Chapter 6 to two of the most urgent issues facing warfighters, decision-makers, and international lawyers today – computer espionage and computer network attacks. Finally, Part IV concludes with a summary of the core principles discussed throughout this book that will serve as the basis for analyzing all use of force issues.
Chapter 2: Military Applications of CyberSpace

CyberSpace is not a physical place – it defies measurement in any physical dimension or time-space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web. Information is the valued commodity of CyberSpace, but nothing actually exists in CyberSpace. When something is said to be in CyberSpace, it is in fact physically resident in a computer or an information system, or it is in transit within a telecommunications infrastructure.

Modern telecommunication systems evolved from the first electric telegraph in 1837\textsuperscript{16} to the first transatlantic cable in 1866,\textsuperscript{17} the first articulating telephone in 1876,\textsuperscript{18} the first wireless telegraph in 1895,\textsuperscript{19} the first commercial public radiotelephone service in 1946,\textsuperscript{20} and the first telecommunications satellite, which was launched by the United States in 1958.\textsuperscript{21} The electronic computer was not invented until 1943, and the ENIAC, the first

\textsuperscript{16} The New York Public Library Desk Reference 129 (1998) [hereinafter NY Public Library Desk Reference].

\textsuperscript{17} Id. at 131.

\textsuperscript{18} Id.

\textsuperscript{19} Id. at 133.


\textsuperscript{21} NY Public Library Desk Reference, supra note 16, at 138.
electronic vacuum tube computer, was built in 1946.22 In the 1950’s IBM imagined a world market for computers and began marketing business computers.23 Finally, in 1975, the world’s first personal computer was announced.24 Computers have evolved from electronic monoliths that were 80 feet long, weighed 30 tons, and had 17,000 tubes, to today’s desktop computers that can store a million times more information than the first computer, and is 50,000 times faster.25

The Internet was originally a network of computers linked by telecommunication infrastructures managed by the U.S. Department of Defense for military and government purposes in the 1970’s.26 Universities and other research facilities soon created their own internal computer networks.27 As these intranets began merging with one another to form a cooperatively-run global collection of computer networks with a common addressing scheme, the Internet was born.28 The World Wide Web refers to a collection of files and databases linked by hypertext that was

22 Id. at 136-37.

23 Levy, supra note 20, at 28, 29.

24 Id.

25 NY PUBLIC LIBRARY DESK Reference, supra note 16, at 109, 146.

26 Id. at 108.

27 Id.

28 Id. at 108, 112.
created in 1989 as the primary platform of the Internet that translates diverse computer protocols into standard format.29

Those who rely upon the benefits of the Internet and the World Wide Web also create vulnerabilities for themselves. The Honorable John J. Hamre, U.S. Deputy Secretary of Defense, has focused on the World Wide Web as “the heart of the Defense Reform Initiative and as key to the reengineering and streamlining of our business practices.”30 He also recognizes, however, that at the same time the Web can also provide our adversaries with a potent instrument to obtain, correlate and evaluate an unprecedented volume of aggregated information regarding DoD capabilities, infrastructure, personnel and operational procedures. Such information, especially when combined with information from other sources, increases the vulnerability of DoD systems and may endanger DoD personnel and their families.31

For example, the memorandum just quoted is publicly available at the Department of Defense (DoD) web site,32 as well as detailed information on the DoD total force anthrax immunization program33 and Operation Desert Fox.34

---

29 Id. at 108, 115. Hypertext is a method of connecting World Wide Web sites through text-based links rather than the menu-oriented systems. Id. at 112.


31 Id.


33 See http://www.defenselink.mil/specials/Anthrax/.
Part I: Introduction

To further demonstrate the information available on the World Wide Web, consider that I found the following aerial photo of my Northern Virginia subdivision in less than ten minutes:35

This photo was taken in 1994 from an altitude of 20,000 feet by a United States Geological Survey aircraft,36 and quality imagery

34 See http://www.defenselink.mil/specials/desert_fox/. The mission of Operation Desert Fox was to strike military and security targets in Iraq that contribute to Iraq’s ability to produce, store, maintain and deliver weapons of mass destruction. Id.

35 See http://www.terraserver.com. Microsoft® TerraServer utilizes georectified digitized aerial photographs from the United States Geological Survey and high-resolution satellite images that are products of a joint Russian/American venture to market declassified satellite photographs from sophisticated Russian mapping satellites.

such as this is available for areas around the world. Access to this type of public information can provide the beginning of a poor-state’s reconnaissance intelligence agency.

In addition to the vulnerabilities posed by publicly available information, states and businesses must also be concerned about those who unlawfully penetrate, or hack into, intranets and computer systems closed to the public. With their open architecture, the Internet and the World Wide Web are ideally suited for asymmetrical warfare and corporate espionage. They can be used by states and nonstate actors to anonymously pry into a state’s public, sensitive, and classified computers; to collect a wide range of government and business information; to manipulate data; to deceive decision makers; to influence public opinion; and to even cause physical destruction from remote locations abroad. An attacking state that understands computers and information systems technology does not need a large land force, a navy to move its forces to hostile shores, or an air force to maintain air superiority over the battlefield to inflict damage on another state. With a few thousand dollars invested in a personal computer, a dedicated and persistent hostile threat can gain access to almost any Internet-linked information infrastructure of any state in the world. The technology of CyberSpace adds new meaning to over-the-horizon warfare. Execution of an organized, large-scale attack can begin anonymously with the stroke of a single key on a computer keyboard, with commands being delivered around the world at the speed of light.

During the military exercise Eligible Receiver in June 1997, for example, the National Security Agency demonstrated that a hostile enemy state could disrupt computer operations at major military commands, cause large-scale blackouts, and interrupt emergency phone service in Washington, D.C., and
several other cities in the United States. Then, in February 1998, two California teenagers with an Israeli mentor broke into sensitive DoD systems and eluded U.S. law enforcement authorities for nearly a month. Although they did not compromise national security or penetrate any classified systems, their attacks were very disturbing because they highlighted sensitive vulnerabilities during the planning for military airstrikes in Iraq.

The Honorable Jamie S. Gorelick, while serving as the Deputy Attorney General of the United States, provided a few other excellent real-world examples that demonstrate the vulnerabilities of governments and businesses:

In 1994, nine people, including an MCI employee, were indicted for a scheme involving a $50-million telephone calling card fraud. Using a sniffer program (which monitors network traffic), they captured and used more than 150,000 calling card numbers. The scheme had been directed by hackers in Germany who then made international calls to attack U.S. computer networks.

A computer hacker broke into files at a bank and a credit union, and then used the information to apply for credit cards in the victim's name. The criminal then used these cards to go on a buying spree. The victim's ability to obtain credit was ruined and had to be painstakingly reestablished.

Con artists have used electronic bulletin board systems to hype recently-purchased penny stocks, driving up the price and giving the con artists a profit.


38 Id.

39 Id.
Between June and October in 1994, approximately 40 wire transfers were attempted from Citibank's cash management system through the use of a computer and phone lines from St. Petersburg, Russia, by compromising the password and user identification code system. Citibank was successful in blocking most of the transfers or recovering the funds from recipient banks, limiting its losses. But the potential loss was enormous.

In 1989, the "Legion of Doom" in Atlanta, Georgia, remotely accessed the administrative computers of Bell South and wiretapped calls and altered phone services. It could have shut down the phone network for the Southeastern United States.

From 1993 to 1995, a man in California gained control of the computers running local telephone switches, and discovered information concerning U.S. government wiretaps conducted pursuant to the Foreign Intelligence Surveillance Act (FISA). He also uncovered a criminal wiretap and warned the target.

In 1992, a computer intruder was arrested for tampering with the Emergency 911 systems in Virginia, Maryland, and New Jersey in order to introduce a virus and bring down the systems.

Also in 1992, a fired employee of an emergency alert network sabotaged the firm's computer system by hacking into the company's computers, causing them to crash for about 10 hours. During that time, there was an emergency at an oil refinery. The disabled system was therefore unable to alert thousands of nearby residents to a noxious release from the refinery.

Finally, a sniffer was introduced into computers of NASA's Goddard Space Flight Center, permitting someone to download a large volume of complex calibration telemetry calculations transmitted from satellites. The sniffer remained undetected for an unprecedented length of time.40

---

Although these vulnerabilities were discovered in the United States, all states share the vulnerabilities of the Internet. To date, it appears that states have only been attacked by recreational and criminal hackers. The Indonesian government, however, is being blamed for a highly-organized attack during January 1999 on non-government computers in Ireland which brought down the East Timor virtual country domain and Internet service to over 3,000 customers. In Executive Order 13010, President Clinton declared that certain “national [commercial] infrastructures are so vital that their incapacity or destruction [by either physical or cyber attack] would have a debilitating impact on the defense or economic security of the United States.” The Executive Order detailed eight categories of critical infrastructures:

- telecommunications;
- electrical power systems;
- gas and oil storage;
- transportation;

41 Email news article from Chris Nuttall, Internet Correspondent, First case of state-sponsored IW? (Jan. 27, 1999) (on file with author).

42 Id.

43 David Hughes, Cyber Raid, Wall Street: This Is No Drill, AVIATION WEEK & SPACE TECHNOLOGY 98 (Dec. 22/29, 1997).
Chapter 2: Military Applications of CyberSpace

- banking and finance;
- water supply systems;
- emergency services (including medical, police, fire, and rescue); and
- continuity of government.

The Executive Order acknowledged that because so many of these critical infrastructures are owned and operated by the private sector, “it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.” A hostile state could correctly assume that a state’s businesses and critical infrastructures are its soft underbelly that is easier to hit than hardened military targets.44

Military applications of CyberSpace are embraced within a broader operational concept coined by the United States as information operations (IO), defined as

Actions taken to affect adversary information and information systems, while defending one’s own information and information systems. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and the interaction of C2 [command and control] with intelligence support. IO are conducted through the integration of many capabilities and related activities. Major capabilities to conduct IO include, but are not limited to, OPSEC [Operations Security], PSYOP [Psychological Operations], military deception, EW [electronic warfare], and physical attack/cess, and could include CNA [Computer Network

44 For a more detailed discussion of Executive Order 13010, evolving concepts of national security, and what the United States has done to date to protect its critical infrastructures, see the think piece entitled Critical Infrastructure Protection: A New Era of National Security provided as Document F of the Document Annex.
Part I: Introduction

Attacks. IO-related activities include, but are not limited to, public affairs (PA) and civil affairs (CA) activities …  

While defensive information operations “ensure the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives,” offensive information operations “are conducted across the range of military operations at every level of war to achieve mission objectives.” Information warfare (IW) is a subset of information operations. IW are those information operations “conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.”

Technology and techniques associated with information systems on the Internet are evolving so rapidly that it is not possible to know the exact nature and magnitude of the threat posed by military applications of CyberSpace. The examples provided in this chapter that depict the attempts and successes of nonstate actors to acquire, disrupt, manipulate, or destroy data are illustrative, however, of the vulnerabilities which can be exploited by states for military or other hostile purposes. The National Security Agency demonstrated during a military exercise that the

---


46 Id. at III-1.

47 Id. at II-1.

United States – and thus, probably all countries – are vulnerable to military applications of CyberSpace, which is simply another medium or environment through which states can either use force or support the use of force. Suffice it to say that the disruption, manipulation, and destruction of data via the Internet promises to be sufficiently disruptive that military applications of CyberSpace are sure to be developed and utilized in the near future. Some, although not all, of these military applications of CyberSpace will rise to the level of a use of force that constitutes an armed attack against a state – and these will be discussed in Part III of this book.
War has existed during the entire history of human society. Indeed, a study in 1968 calculated “that there had been only 268 years free of war in the previous 3,421.” From the organized food-gathering and wife-seeking raids of primitive man, to the Persian Wars of the fifth century B.C. and the Second World War of the twentieth century, war was accepted as a legitimate form of violence. Although another study in 1998 reflects a continued downward trend for armed conflicts since 1989, it estimates that there were still 25 major armed conflicts ongoing in
While only the conflict between India and Pakistan was interstate, other states supported at least one party in these intrastate conflicts.\textsuperscript{55}

Motives for war were wide-ranging, and included the acquisition of territory, the domination of another people, the access to scarce resources, glory, prestige, and revenge.\textsuperscript{56} Other motivations included the desire to pillage, rape, and murder because war was simply a culture and a way of life for some peoples, such as the Cossacks.\textsuperscript{57} In many respects, war simply began as organized armed robbery by plundering hordes among dissimilar peoples and tribes.\textsuperscript{58}

The law of conflict management, \textit{jus ad bellum}, is a set of rules that govern the resort to armed conflict and determine whether the conflict is lawful or unlawful in its inception.\textsuperscript{59} A study of the law of conflict management is central to understanding what is considered a use of force under international law because war is the legal consequence of a use of force by one state against

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{55} Id.
\item \textsuperscript{56} \textit{See} Preston & Wise, supra note 50, at 5-6.
\item \textsuperscript{57} \textit{See} John Keegan, A History of Warfare 7-9 (1993).
\item \textsuperscript{58} Lothar Kotzsch, The Concept of War in Contemporary History and International Law 25 (1956).
\item \textsuperscript{59} Documents on the Laws of War, supra note 2, at 2-3.
\end{itemize}
\end{footnotesize}
another.\textsuperscript{60} For four millennia, the \textit{jus ad bellum} generally allowed states to engage in war at any time; however, virtually every recorded civilization developed some rules governing the initiation of war.\textsuperscript{61} The Egyptians and the Sumerians developed rudimentary \textit{jus ad bellum} during the second millennium B.C.\textsuperscript{62} As a general rule, the Hittites of the fourteenth century B.C. formally exchanged letters and demands before commencing hostilities.\textsuperscript{63}

During the approximate period 335 B.C. to A.D. 1800, war was examined on a moral, philosophical level that approved of war if the cause was just.\textsuperscript{64} This philosophy of war as an instrument of justice was replaced in the early 1800s by the acceptance of war as a political instrument of national policy.\textsuperscript{65} The Prussian philosopher and military theorist General Carl von Clausewitz is

\textsuperscript{60} See The Prize Cases, 67 U.S. (2 Black) 635 (1862), excerpted in \textit{National Security Law} 78, 78-80 (Stephen Dycus et al. eds.) (1997) [hereinafter \textit{National Security Law (Dycus et al.)}]. In this 1862 case, the United States Supreme Court defined war under the law of nations as "[t]hat state in which a nation prosecutes its right by force."

\textsuperscript{61} \textit{1 The Law of War: A Documentary History} 3 (Leon Friedman ed., 1972).

\textsuperscript{62} \textit{Id.}

\textsuperscript{63} \textit{Id.}

\textsuperscript{64} \textit{National Security Law} 51-57 (John Norton Moore et al. eds., 1990) [hereinafter \textit{National Security Law (Moore et al.)}].

\textsuperscript{65} \textit{Id. at 57}. Chapter 3 of this text provides a more detailed discussion of the development of the law of conflict management divided into six approximate time periods: (1) just war, 335 B.C. to A.D. 1800; (2) war as fact, 1800-1918; (3) early League of Nations, 1919-1925; (4) Kellogg-Briand Pact and late League, 1928-1945; (5) early United Nations Charter, 1945-1958; and, (6) contemporary Charter, 1959-present.
often quoted as describing war as the continuation of national policy by other means.66 Two fundamental tenets of Clausewitz’s philosophy are the legitimacy of war as a normal phase in the relations among states and the absolute sovereignty of states.67

The first attempt to place juristic restrictions on this freedom to resort to war did not begin until the Hague Peace Conferences of 1899 and 1907.68 Article 1 of the 1907 Hague Convention III, for example, required parties to present a “previous and explicit warning, in the form either of a declaration of war, giving reasons, or of an ultimatum with conditional declaration of war.”69 This was nothing more, however, than a formal recognition

66 See, e.g., Keegan, supra note 57, at 3 (While noting that variations of the concept that war is the continuation of policy by other means is frequently quoted, Keegan challenges the simplicity of the translation. The original German, Keegan explains, expresses a more subtle and complex idea that “war is the continuation ‘of political intercourse’ … ‘with the intermixing of other means’ … ‘”’); National Security Law (Moore et al.), supra note 64, at 57 (“War is only a part of political intercourse… . War is nothing but a continuation of political intercourse, with a mixture of other means.”); U.S. Marine Corps, FMFM 1, Warfighting 19 (1989) (“War does not exist for its own sake. It is an extension of policy with military force.”). General Carl von Clausewitz (1780-1831) served as the director of the War College in Berlin from 1818 to 1830 where he began his work on his 3-volume masterpiece On War, which was published posthumously in 1832. Karl von Clausewitz, Microsoft Encarta ’95 (CD-ROM Multimedia Encyclopedia, 1994).


that the resort to war was legal.  

Similarly, the series of nineteen Bryan Treaties concluded by the United States and a number of other states between 1913 and 1916 imposed an obligation on contracting parties to submit all of their disputes to a conciliation commission, and not to begin hostilities prior to the commission’s report.

After World War I, the League of Nations also attempted to restrict the right of states to resort to war. As in the Bryan Treaties, members of the League of Nations were required to submit their disputes to judicial settlement, arbitration, or to the Council of the League, and were prohibited to begin war within a period of three months from the judicial decision, arbitral award, or the Council’s report. The only prohibition on the resort to war was against any state that complied with the judicial decision, arbitral award, or a unanimous decision of the Council.

The League of Nations was unsuccessful in its attempt to prohibit or, in practice, restrict the resort to war. The international community attempted to correct the shortcomings of the League of Nations by adopting the 1924 Geneva Protocol for the Pacific

---


71 Id. at 109-10.

72 Id. at 110.

73 Id.

74 Id.

75 Id.
Part II: The Law of Conflict Management – The Legacy of War

Settlement of International Disputes. This Protocol prohibited the resort to war except in self-defense or in the case of collective enforcement measures, but it never became binding law.

The decisive turning point in the history of the *jus ad bellum* was the adoption of the Briand-Kellogg Pact on August 27, 1928. Article 1 of this Pact provides that “[t]he High Contracting Parties solemnly declare in the names of their respective peoples that they condemn recourse to war for the solution of international controversies and renounce it as an instrument of national policy in their relations with one another.” Nearly all existing states of the time became parties to the Briand-Kellogg Pact, and it soon became customary international law. Despite its significance in principle, the Pact had its weaknesses. Most notably, it merely prohibited war and not the use of force, allowing states to engage in devastating hostilities while claiming no offenses under the Pact were being committed.

---

76 Id.

77 Id.

78 Id.


81 See id.

82 Id. at 111.
Chapter 3: The U.N. and Contemporary *jus ad bellum*

**Contemporary *jus ad bellum***

Article 2(4) of the Charter of the United Nations\(^{83}\) was the *coup de grâce* for the theory and practice of the *jus ad bellum* that recognized the right of states to resort to war. This article requires all Member States to “refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state … .”\(^{84}\) The Charter clearly outlaws the aggressive use of force\(^{85}\) while recognizing a state’s inherent right of individual and collective self-defense in Article 51 and the Security Council’s obligation under Article 39 to maintain or restore international peace and security. **Articles 2(4), 39, and 51 of the Charter now redefine and codify the contemporary *jus ad bellum* in its entirety.**\(^{86}\) If a state activity is a use of force within

---


\(^{84}\) U.N. CHARTER art. 2(4).

\(^{85}\) Generally, aggressive refers to beginning a dispute by being the first to either threaten or use force. See BLACK’S LAW DICTIONARY, supra note 15, at 60. However, an aggressive use of force, *i.e.*, aggression, is not defined by the Charter, and despite fifty-four years of efforts, the international community has failed to formulate a generally acceptable definition of aggression. See generally, e.g., ANN VAN WYVEN THOMAS AND A.J. THOMAS, JR., THE CONCEPT OF AGGRESSION IN INTERNATIONAL LAW (1972). Accordingly, an aggressive use of force can best be identified by studying state practice. For the purposes of this book, an *‘aggressive use of force’* is a shorthand term used to refer to any use of force within the meaning of Article 2(4) that is not justified by a state’s right of self-defense or authorized by the Security Council under its coercive Chapter VII powers. While this definition is somewhat circular in its reasoning, it is useful shorthand to facilitate a discussion of the basic principles of international law necessary for the more detailed discussion in Parts III and IV of this book that define heuristically what state activities constitute an aggressive use of force.

\(^{86}\) See THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 111.
the meaning of Article 2(4), it is unlawful unless it is an exercise of that state’s inherent right of self-defense or unless it is authorized by the Security Council under its coercive Chapter VII authority.

With the creation of the Charter norm prohibiting the right of states to resort to the aggressive use of force, the historical concept of the *jus ad bellum* evolved to one of the *jus contra bellum*, i.e., the law against the aggressive use of force.\(^{87}\) The underlying principle of the *jus contra bellum* is now penal law\(^ {88}\) that prohibits all aggressive use of force while retaining a state’s right of individual and collective self-defense. The aggressive use of force by a state is now a crime against peace that has been outlawed by the international community.\(^{89}\) Accordingly, international law imputes individual criminal responsibility for those who operate at a policy-decision level of an aggressor state.\(^{90}\)

---

\(^{87}\) KOTZSCH, *supra* note 58, at 83.

\(^{88}\) *Id.*


\(^{90}\) *E.g.*, NATIONAL SECURITY LAW (Moore et al.), *supra* note 64, at 369-70, which quotes the opinion of the International Military Tribunal in *U.S. v. Leeb (The High Command Case)* at 370:

If and as long as a member of the armed forces does not participate in the preparation, planning, initiating, or waging of aggressive war on a policy level, his war activities do not fall under the definition of crimes against peace.
for a crime against peace; *i.e.*, the “planning, preparation, initiation or waging of a war of aggression, or a war in violation of international treaties, agreements or assurances, or participation in a common plan or conspiracy for the accomplishment of any of the foregoing … ”

Articles 2(4), 39, and 51 must be read together to determine the scope and content of the Charter’s prohibition on the aggressive use of force, the responsibility of the Security Council to enforce this prohibition, and the right of all states to use force in self-defense. Article 2(4) of the Charter prohibits the threat or use of force by any state against the territorial integrity or political independence of another state except in individual or collective self-defense as authorized by international law and recognized by Article 51 of the Charter. Articles 2(4) and 51 provide:

\[
\text{Article 2} \\
\text{The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles: …} \\
\text{(4) All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.}
\]

---


93 See NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 85.
Article 51

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.93

Article 2(4) is so important to the maintenance of international peace and security, it has been described by one scholar as a “critical legal obligation” outlawing aggressive war that permits no derogation and as “the single most important fundament of world order … ”94 Article 51 is equally important, because it recognizes the distinction between an unlawful, aggressive use of force and a lawful, defensive use of force that is the inherent right of all states.95 Both Articles 2(4) and 51 are customary international law.96

93 U.N. CHARTER arts. 2(4), 51.


95 Id. at 151.

Self-defense and the use of force by states

It is a fundamental principle of the contemporary law of conflict management that states may only use force lawfully in individual or collective self-defense. States recognize this principle, and have invoked their right of self-defense as justification for almost every use of force since the Charter has been in effect.97 Since the text of Article 51 recognizes this right of self-defense at the time an armed attack occurs, the pivotal focal point of any self-defense analysis is on the meaning of an armed attack.98 It is generally accepted, however, that the Article 51 right of self-defense is coextensive with a state’s right under customary international law.99 The remainder of this section will detail the basic rules of self-defense necessary for a full understanding of what self-defense options are available as a matter of international law should an armed attack occur. Chapter 6, infra, will analyze in detail what state activities constitute a use of force that rises to the level of an armed attack.

Necessity and proportionality

Customary international law requires that all uses of force be necessary and proportional,100 and it prohibits the use of force

97 See id. at 663.

98 See id.

99 Moore, supra note 94, at 151. But see The Charter of the United Nations: A Commentary, supra note 68, at 666, which concludes that Article 51 excludes any right of self-defense “other than that in response to an armed attack.”

100 Moore, supra note 94, at 156.
for retaliatory or punitive actions.\textsuperscript{101} The principles of necessity and proportionality apply under both the law of conflict management and the law of armed conflict. The law of conflict management requires that a state’s use of force be necessary for either individual or collective self-defense.\textsuperscript{102} For example, the requirement of necessity for the international community to use force in collective self-defense was clearly met when Iraq invaded and brutally occupied Kuwait in 1990.\textsuperscript{103} If Iraq had simply entered Kuwait, destroyed a number of its oil fields, and then quickly left, the principle of necessity would very likely not have justified the use of force in the absence of a continuing threat.

Similarly, the law of conflict management requires that a state’s use of force be proportional in intensity and magnitude to what is reasonably necessary to promptly secure the permissible objectives of self-defense.\textsuperscript{104} It is “emphatically not a requirement that the defense limit itself to weapons systems employed by the aggressor or to employ force only at levels employed by the aggressor or to employ force only at levels sufficient to be ineffectual.”\textsuperscript{105} Indeed, during a debate on the Viet Nam War, one noted scholar concluded that if a state party to an armed conflict has greater military resources potentially available to it, an

\begin{itemize}
\item \textsuperscript{101} \textit{The Charter of the United Nations: A Commentary, supra} note 68, at 677.
\item \textsuperscript{102} \textit{See Moore, supra} note 94, at 156-57.
\item \textsuperscript{103} \textit{Id.} at 157.
\item \textsuperscript{104} \textit{Id.} at 158.
\item \textsuperscript{105} \textit{Id.}
\end{itemize}
insufficient use of force by that state to end the war quickly would violate general norms of international law.\textsuperscript{106}

A necessary use of force is defined by the law of armed conflict as only

that degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy with a minimum expenditure of time, life, and physical resources ... \textsuperscript{107}

Similarly, the law of armed conflict defines a proportional use of force as that level of force required to destroy a military objective\textsuperscript{108} but which does not cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians.\textsuperscript{109}

\textsuperscript{106} \textit{Id.} at 181 n.38.


\textsuperscript{108} Lawful military objectives include combatants and those objects which, by their nature, location, purpose, or use, effectively contribute to the enemy’s war-fighting or war-sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack.

\textit{Id.} ¶ 8.1.1.

\textsuperscript{109} \textit{Id.} ¶ 8.1.
The principle of proportionality is frequently misunderstood as limiting the use of force that can be used to destroy a military objective to the strength or firepower of that objective – or in some other way limiting the use of force between combatants. It does not, however, require any such parity of force. Proportionality is a limitation on the use of force against a military objective only to the extent that such a use of force may cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians. The principle of proportionality is a balancing of the need to attack a military objective with the collateral damage and human suffering that will be caused to civilian property and civilians by the attack. Categorically, proportionality imposes no limitations on the use of force between combatants in the absence of any potential effect on civilians or civilian property.\textsuperscript{110}

\textit{Collateral damage and injury to civilians}

Proportionality limits the amount of force that can be used to destroy a military objective to that which does not cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians. It does not prohibit any damage to civilian property or injury to civilians. If civilian property and civilians support a war effort, they are subject to

attack, and they are subject to incidental damage during an attack on a lawful military objective. These two corollaries to the principles of necessity and proportionality are very important to highlight in the context of the impact of state activities on civilian property and civilians.

While civilian property and civilians may not be the object of an attack as such, states may use force against civilian property and activities that support or sustain an enemy state’s warfighting capability during armed conflict. States may use force during armed conflict, for example, against economic targets such as enemy lines of communication, rail yards, bridges, rolling stock, barges, industrial installations producing warfighting products, and power generation plants. In today’s modern society, much of a state’s civilian infrastructure is used for military purposes, and is thus subject to lawful attack during armed conflict if there is a military advantage to be gained by such an attack.

In its final report to Congress on the conduct of the Persian Gulf War, the U.S. Department of Defense noted that

[a] bridge or highway vital to daily commuter and business traffic can be equally crucial to military traffic, or support for a nation’s war effort. Railroads, airports, seaports, and the interstate highway system in the United States have been funded by the Congress in part because of US national security concerns, for example, each proved invaluable to the movement of US military units to various ports for deployment to

111 COMMANDER’S HANDBOOK, supra note 107, ¶ 8.1.2.

112 Id. ¶ 8.1.1.

113 CONDUCT OF THE PERSIAN GULF WAR: FINAL REPORT, app. Q, supra note 110, at 10, 11.
Southwest Asia (SWA) for Operations Desert Shield and Desert Storm. Destruction of a bridge, airport, or port facility, or interdiction of a highway can be equally important in impeding an enemy’s war effort.

The same is true with regard to major utilities; for example, microwave towers for everyday, peacetime civilian communications can constitute a vital part of a military command and control (C2) system, while electric power grids can be used simultaneously for military and civilian purposes.\textsuperscript{114}

A state has always been dependent upon its private industry to support its war efforts, and to the extent private industry supported a war effort, it has always been a lawful target under the law of armed conflict. Technology, however, is increasing the interdependence of a state’s commercial sector with its government functions, making more and more of the civilian infrastructure subject to lawful attack during armed conflict. Except for shipping, private industry may also be well protected within a state’s borders. Unfortunately, technology such as computers and the Internet is also making the civilian infrastructure far more accessible and vulnerable to attack than ever before.

Furthermore, it is not unlawful to cause \textit{incidental} injury to civilians, or collateral damage to civilian property, during an attack on a legitimate military objective.\textsuperscript{115} The balancing of proportionality does require, however, that such incidental injury or collateral damage not be excessive in light of the advantage anticipated by the attack.\textsuperscript{116} The law of armed conflict requires a

\begin{itemize}
\item[\textsuperscript{114}] Id.
\item[\textsuperscript{115}] COMMANDER’S HANDBOOK, supra note 107, ¶ 8.1.2.
\item[\textsuperscript{116}] Id.
\end{itemize}
military commander to take all reasonable precautions, based upon all the facts known or reasonably available at the time, to keep civilian casualties and damage to the minimum consistent with mission accomplishment and the security of his or her personnel.\footnote{Id.}

\textit{Anticipatory self-defense}

There is no consensus over the point in time at which self-defense against an armed attack may be taken.\footnote{Id.} Some scholars conclude that the customary international law right of anticipatory self-defense is incorporated by Article 51, while others conclude that an anticipatory right is contrary to Article 51.\footnote{The Charter of the United Nations: A Commentary, supra note 68, at 675-76.} Opposing schools of thought, however, usually converge when applied to a given set of facts. Anticipatory self-defense authorizes the use of force in self-defense at a point in time \textit{before} an attack occurs. As defined by then Secretary of State Daniel Webster in the \textit{Caroline} case, this point in time occurs when “the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation.”\footnote{Id. at 675.} One opponent of anticipatory self-defense concludes that Article 51 requires that an armed attack occur – but he also concludes that self-defense is “permissible only after the armed attack has already been launched.”\footnote{Id. at 676.} The fact that
this opponent acknowledges that force may be used in self-defense before the attack occurs but after it is launched acknowledges the existence of the right of anticipatory self-defense by his very argument. The real debate is not over whether the right of anticipatory self-defense exists, but to what extent it exists under the conditions of the *Caroline* case.

**Articles 2(4) and 51: Closing the gap**

The thresholds of Articles 2(4) and 51 are different in scope; *i.e.*, the Article 2(4) concept of a threat or use of force is much broader than the more restrictive Article 51 threshold of armed attack.\footnote{See id. at 663.} This correct observation, however, causes one author to arrive at the “stunning conclusion” that an *unlawful* use of force that does not meet the threshold of an armed attack does not give the victim state the right to respond with a *use of force*.\footnote{Id. at 663-64.} If this conclusion simply means that the right to self-defense is invoked somewhere along the spectrum of state activities between threats of force and the actual use of force, then it is a reasonable interpretation of Articles 2(4) and 51. After all, the low threshold of Article 2(4) includes mere verbal threats, and international law requires that all uses of force, including those in self-defense, to be necessary and proportional. Accordingly, such an interpretation does not prohibit a use of force in self-defense in response to a minor use of force that occurs over a very short period of time, but the right of self-defense under customary international law may not justify an armed response.

In sharp contrast, if this “stunning conclusion” means that states do not always have the right, albeit limited to narrowly
circumscribed situations, to use necessary and proportional force in self-defense, it is highly unacceptable – and in practice, it has not been accepted by any consensus of states. Notwithstanding the purposes and principles of the Charter and the very worthwhile goal of international peace and security, international law does not create a situation where a state must sit idly by while another state uses unlawful force against it. To do so would undermine international peace and security by allowing states to unlawfully use force with impunity and to gain from their unlawful actions.

It is not clear textually just how large a gap may exist between the two thresholds. In practice, the analysis within this gap focuses on what is a lawful, defensive response to an unlawful use of force. For example, if one state unlawfully uses force by using a single missile to destroy a telecommunications tower just across its border that was broadcasting unwanted pop videos into its territory, the victim state could use force in self-defense by shooting down the incoming missile. Once the missile strike occurs, however, international law would prohibit a punitive use of force in retaliation for the strike. An appropriate response by the territorial state after such an isolated missile strike would be to seek civil redress.

Similarly, consider a situation where one state admittedly uses armed military force to rescue its nationals whose lives are in danger, and does so over the objection of the territorial state. Chapter 6, infra, concludes that this is a use of force within the meaning of Article 2(4) that is a lawful act of self-defense. The rescue operation, however, is very short in duration – perhaps less than an hour. Once the rescue operation is completed, the situation exists where a use of force has occurred, but the territorial state has no right to respond with force in self-defense because the rescue
operation is now complete. An appropriate response by the territorial state after the rescue operation would be to publicly renounce the rescue operation.

In contrast, consider a pattern of missile attacks by a state that originate from the same launch site. In addition to having the right to shoot down incoming missiles in self-defense, the victim state also has the right of anticipatory self-defense to preemptively destroy the launch site to prevent future attacks.

Those who embrace such a patently unreasonable conclusion that “any state affected by another state’s unlawful use of force not reaching the threshold of an ‘armed attack,’ is bound, if not exactly to endure the violation, then at least to respond only by means falling short of the use or threat of force, which are thus often totally ineffective” frequently temper their harsh norm by their interpretations of the definitions of use of force and armed attack. For example, one scholar concludes it is within a state’s lawful discretion to deny transit rights to a land-locked state. In extreme cases, however, the same scholar concludes that such a denial may lead “to an impairment equating to a military invasion (e.g., by cutting off all communications routes) [and that] an ‘armed attack’ can be taken to exist.” This is a very interesting conclusion, since such a denial is the exercise of a state’s lawful

124 The justification for a territorial state to use armed force during the rescue operation is discussed in Chapter 6 under the section concerning the protection of nationals abroad.

125 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 663-64 (emphasis added).

126 Id. at 670.

127 Id.
right to exclude others from its territory. Similarly, the same scholar concludes that the use of armed force by a state against commercial vessels and aircraft of another state is not an armed attack, unless it is on the whole of the fleets.128

Frequently, but not always, the end result of the application of the harsh norms is simply an analysis of what is a necessary and proportional response in self-defense. The same scholar who makes the exceptions discussed above nevertheless concludes that “forcible rescue operations for nationals endangered in another country are no longer lawful under the U.N. Charter.”129 In the final analysis, armed force is interpreted very broadly to include non-military physical force and indirect force that includes the passive acquiescence of the use of a state’s territory by a belligerent.130

Also consider the conclusion of another scholar who interprets a use of force to be the same as an armed attack. He concludes that a use of force must reach a certain “gravity” and that minor frontier incidents are not per se uses of force that rise to the Article 2(4) threshold because “the minor nature of an attack is prima facie evidence of absence of intention to attack, of honest mistake, or simply the limited objectives of an attack.”131 His explanation also returns the analysis to the issue of what is a necessary and proportional response in self-defense under the circumstances.

128 Id. at 671.

129 Id. at 672.

130 Id. at 111-13.

131 See BROWNLE, supra note 89, at 366.
The principle that a state never loses its right of self-defense may be inconsistent with the views of some, but it is consistent with state practice and the following *dicta* found in the *Nicaragua* judgment of the International Court of Justice:

> Since the Court is here dealing with a dispute in which a wrongful use of force is alleged, it has primarily to consider whether a State has a right to respond to intervention with intervention going so far as to justify a use of force in reaction to measures which do not constitute an armed attack but may nevertheless involve a use of force. … However, since the Court is bound to confine its decision to those points of law which are essential to the settlement of the dispute before it, it is not for the Court here to determine what direct reactions are lawfully open to a State which considers itself the victim of another State’s acts of intervention, possibly involving the use of force. … *It might however be suggested that, in such a situation, the United States might have been permitted to intervene in Nicaragua in the exercise of some right analogous to the right of collective self-defence, one which might be resorted to in a case of intervention short of armed attack.*

Accordingly, *a state never loses its right to use force in self-defense in response to a use of force within the meaning of Article 2(4), however, the right of self-defense under customary international law may not always justify an armed response.* This is a very important point of international law to remember throughout any discussion of a state’s right of self-defense – although a state never loses its right to use force in self-defense,

---

the principles of necessity and proportionality may not justify the use of force in self-defense.

**Security Council authority to use force**

As an exercise of the international community’s inherent right of collective self-defense, Article 39 of the Charter imposes an obligation on the Security Council to maintain international peace and security. Article 39 provides that

> The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.\(^{133}\)

Decisions taken by the Security Council under Article 39 are binding on all Member States.\(^{134}\) Every threat or use of force proscribed by Article 2(4) is, *per se*, a threat to international peace and security within the meaning of Article 39.\(^{135}\) Accordingly, the Security Council has the coercive authority to authorize the use of force in response to any violation of Article 2(4).\(^{136}\)

The authority of the Security Council to use force, however, extends beyond violations of Article 2(4). Indeed, the

\(^{133}\) U.N. Charter art. 39.


\(^{136}\) *Id.*
Article 39 threshold extends considerably below the Article 2(4) threshold,\textsuperscript{137} giving the Security Council the power to authorize states to use force under circumstances where states do not independently have the right to use force in self-defense. For example, scholars have concluded that threats to the peace within the meaning of Article 39 include extreme intrastate violence or human rights violations, the failure of a state to surrender terrorists in accordance with the order of the Security Council, an illegal racist regime, cross-frontier expulsion of refugees, diversion of a river by an up-stream state, and serious violations of international law that may provoke an armed response.\textsuperscript{138}

Article 41 authorizes the Security Council to shape an international community response to a threat to international peace and security that falls short of deploying military forces under Article 42. This article provides that

\begin{quote}
The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.\textsuperscript{139}
\end{quote}

It is very important to emphasize two aspects of Article 41 that are frequently overlooked or misunderstood. First, Article 41 is an explicit recognition that the Security Council has the authority to require Member States to cease any or all forms of economic

\textsuperscript{137} Id.

\textsuperscript{138} Id. at 113, 611-12.

\textsuperscript{139} U.N. CHARTER art. 41.
relations, communications, or diplomatic relations with a state to coerce that state to conform to internationally accepted standards of behavior. Its authority is directed toward Member States, not the state that has created a threat to international peace and security. Second, Article 41 does not provide that the enumerated examples may not constitute a use of force within the meaning of Article 2(4). It simply provides that they are ‘measures not involving the use of armed force’ that states can be required to employ in contrast to measures involving the use of armed force in Article 42 that the Security Council does not have the authority to require Member States to deploy. As discussed in Chapter 6, infra, political and economic coercion may be a use of force within the meaning of Article 2(4) which may constitute an ‘armed attack’ within the meaning of Article 51, thus invoking a state’s right of self-defense.

In contrast, Article 42 authorizes the Security Council to conduct or authorize belligerent military operations against an aggressor state when such actions are necessary to maintain or restore international peace and security. This article provides that

Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.¹⁴⁰

In contrast to Article 41 which explicitly authorizes the Security Council to require Member States to enforce economic and political sanctions against an aggressor state, Article 42 only

¹⁴⁰ U.N. CHARTER art. 42.
permits the Security Council to authorize Member States to use armed military force against an aggressor state.141

Conclusion

There is no black and white, mechanical rule in the law of conflict management that clearly defines what a use of force is under all circumstances. What constitutes a prohibited ‘threat or use of force’ is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances. Such a question of fact defies rote, categorical definition. For example, a state’s activity that is lawful against another state of equal size may nevertheless be significant enough against a smaller state to cross Article 2(4)’s “political independence” threshold. Accordingly, a state’s activities in CyberSpace, like all of its activities anywhere else, must be analyzed within the framework of the law of conflict management and state practice.

Figure 1 graphically depicts the interrelationships of Articles 2(4), 39, 41, 42, and 51. This figure will serve as the foundation upon which a model will be built in later chapters to analyze use of force issues. It highlights along the spectrum of interstate relations the varying thresholds of Articles 2(4), 39, and 51. It also portrays graphically the corresponding rights of states to use force in self-defense and the authorities of the Security Council to take actions to maintain international peace and security.

Chapter 3: The U.N. and Contemporary Jus ad Bellum

**The Charter Jus ad Bellum Paradigm**

© 1998 Walter Gary Sharp, Sr.

Figure 1

**Spectrum of Interstate Relations**

- **Art. 39**: Threat to the peace
- **Art. 2(4)**: Threat of force
- **Art. 51**: Armed attack (use of force)

**UNSC** may require states to comply with Art. 41 measures

Any measures or use of force authorized by the UNSC under Chapter VII

Diplomatic measures; severance of diplomatic relations; complete or partial interruption of economic relations or interstate communications; arbitration, judicial proceedings, etc.
This chapter was intended to provide a historical context and an understanding of the basic principles of the law of conflict management. A detailed analysis of how the law of conflict management and state practice defines a use of force and an armed attack is provided in Chapter 6, infra. During all subsequent discussions of the law of conflict management, it must be remembered that although a state never loses its right to use force in self-defense in response to a use of force within the meaning of Article 2(4), the right of self-defense under customary international law may not always justify an armed response.
Chapter 4: The Common Article 2 Threshold

Evolution and significance of the threshold

The law of war, *jus in bello*, also commonly referred to as the law of armed conflict, governs the actual conduct of hostilities and has developed as customary international law through the practice of almost all societies over thousands of years – from the era of the Greeks and Romans to the Middle Ages and the twentieth century.\(^{142}\) The practice of codifying the law of armed conflict in binding international agreements began in the nineteenth century with the 1856 Paris Declaration on Maritime War.\(^{143}\) Codification accelerated at the turn of the twentieth century,\(^{144}\) and the law of armed conflict has generally developed in two regimes: the Hague regulations that govern the means and methods of warfare, and the Geneva conventions that govern the protection of victims of war.\(^{145}\)

\(^{142}\) DOCUMENTS ON THE LAWS OF WAR, supra note 2, at 1-2; 1 THE LAW OF WAR: A DOCUMENTARY HISTORY, supra note 61, at 3.

\(^{143}\) DOCUMENTS ON THE LAWS OF WAR, supra note 2, at 2-4.

\(^{144}\) Id. at 3.

\(^{145}\) See generally DOCUMENTS ON THE LAWS OF WAR, supra note 2. Nevertheless, despite the development of these extensive regimes and the threat of prosecution, barbaric cruelty remains a characteristic of twentieth century warfare. One study commissioned in 1913 by the Carnegie Endowment for International Peace recorded the atrocities among the Turks, Serbs, and Greeks during the Balkan war that ended in the early twentieth century:

These soldiers all state that everywhere they burned the Bulgarian villages. Two boast of the massacre of prisoners of war. One remarks that all the girls they met with were violated. Most of the letters dwell on the slaughter of noncombatants, including women and children. “Here we are burning the villages and killing the Bulgarians, both women and children.
Most notable of the regime of Geneva conventions are the four Geneva Conventions of 1949 developed at the initiative of the International Committee of the Red Cross (ICRC). ¹⁴⁶ These four

We picked out their eyes (five Bulgarian prisoners) while they were still alive.” … From Kukush to the Bulgarian frontier the Greek Army devastated the villages, violated the women and slaughtered the noncombatant men.

United States v. List, 11 TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS 759, 1218-19 (1950). Even during the war in the Balkans that began in 1992, as many as 100,000 women were taken hostage and systematically raped in an effort to defile and impregnate them so they would not be accepted back into their community. Patricia Forestier, Psychiatric Genocide! How the Barbarities of ‘Ethnic Cleansing’ Were Spawned by Psychiatry, FREEDOM, May 1993, at 6, 6-11, 34-35. Other atrocities included soldiers who burned families alive in their homes, crushed the heads of young children, and raped pregnant mothers in front of their families. Rod Nordland, ‘Let’s Kill the Muslims!’, NEWSWEEK, Nov. 8, 1993, at 48, 48-49.

All of these and many other atrocities are clearly prohibited by the jus in bello. Their continued existence is not a failure of the rule of law, but a failure of the international community to enforce the law. Despite the serious war crimes that were committed during a number of international armed conflicts such as Korea, Vietnam, Palestine, Pakistan-Bangladesh-India, Cyprus, Lebanon, and the Persian Gulf, the international community remains reluctant to take war crimes prosecutions seriously. The creation and work of the International Criminal Tribunal for the former Yugoslavia and the recent developments on an International Criminal Court are hopeful steps.

conventions apply during international armed conflict, and deal with the following four categories of victims of war, respectively: wounded and sick in armed forces in the field; wounded, sick and ship-wrecked in armed forces at sea; prisoners of war; and civilians. The four Geneva Conventions of 1949 are adhered to by more states than any other agreements on the laws of armed conflict and are declaratory of customary international law.

These conventions are linked by certain general principles and by common articles that are found throughout each of the four conventions. Common Article 2 governs the application of the four Geneva Conventions of 1949 and is widely accepted as the threshold test for when an international armed conflict exists, and consequently, the application of the law of armed conflict in its entirety.

Common Article 2 is thus the transition point between peace and armed conflict that determines when the law of armed
conflict applies. This transition point which determines when an armed conflict begins under the Common Article 2 threshold corresponds to the Charter’s Article 51 threshold of an armed attack. Consequently, an understanding of the Common Article 2 threshold helps to define what is a use of force and an armed attack under the law of conflict management.

**Defining an armed attack**

Common Article 2 invokes the provisions of the Conventions upon one of three factual conditions. Accordingly, an international armed conflict exists upon the declaration of war, the occurrence of “any other armed conflict” between two or more contracting parties even if the state of war is not recognized by one of them, and in all cases of partial or total occupation even if met with no armed resistance.\(^{151}\) The existence of international armed conflict and the corresponding application of the law of armed conflict in cases of declared war\(^{152}\) or occupation\(^{153}\) is normally self-evident.


\(^{152}\) Although a declaration of war is not required to establish the existence of international armed conflict, such a declaration does define a legal state of armed hostilities between states even in the absence of the use of force. U.S. DEP’T OF THE ARMY, *FIELD MANUAL 27-10, THE LAW OF LAND WARFARE*, ¶ 8 (1956) [hereinafter FM 27-10].

\(^{153}\) Military occupation is a question of fact that “presupposes a hostile invasion, resisted or unresisted, as a result of which the invader has rendered the invaded government incapable of publicly exercising its authority, and that the invader has successfully substituted its own authority for that of the legitimate government in the territory invaded.” *Id.* ¶ 355.
Although the terms ‘war’ and ‘armed conflict’ are frequently used interchangeably and refer to a state of hostilities that invokes the law of armed conflict, war refers to a state of *de jure* hostilities invoked by a formal declaration of one party\(^{154}\) that creates an international armed conflict as a matter of law.\(^{155}\) In contrast, ‘any other armed conflict’ refers to a state of *de facto* hostilities invoked by the use of force by one party without any formal declaration of war.\(^{156}\) Under exceptional circumstances, such as the invasion of Kuwait by three Iraqi Republican Guard Forces Command divisions on August 2, 1990,\(^{157}\) *de facto* hostilities may also be self-evident. Without such exceptional circumstances, however, determining when “*any other armed conflict*” exists is a factual, subjective determination that centers on the use of force between two states.

The commentary of the 1949 Geneva Convention No. IV published by the ICRC describes the Common Article 2 threshold for *de facto* hostilities as follows:

> *Any difference* arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies

\(^{154}\) DOCUMENTS ON THE LAWS OF WAR, *supra* note 2, at 1-2.

\(^{155}\) FM 27-10, *supra* note 152, ¶ 8. For an excellent historical discussion of the evolution and meaning of *de jure* and *de facto* wars, see KOTZSCH, *supra* note 58, at 36-65.

\(^{156}\) DOCUMENTS ON THE LAWS OF WAR, *supra* note 2, at 1-2.

the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place.\textsuperscript{158}

Although not very clearly defined, this explanation depicts a low Common Article 2 threshold for the application of the Conventions designed to afford maximum protection to non-belligerents and belligerents by ensuring the Conventions apply to as many hostile interventions between the members of the armed forces of two states as possible.\textsuperscript{159}

This ICRC Commentary of Common Article 2 does offer, however, three criteria that add structure to a factual analysis of the existence of \textit{de facto} hostilities. The emphasized terms ‘[a]ny difference’, ‘no difference how long the conflict lasts’, and ‘no difference … how much slaughter takes place’ provide that the \textit{scope}, \textit{duration}, and \textit{intensity} of a use of force between the members of the armed forces of two states are the central factors in determining the existence of \textit{de facto} hostilities. \textbf{Based upon this ICRC Commentary of the Common Article 2 threshold, \textit{de facto} hostilities exist, and consequently, the \textit{jus in bello} applies, when any use of force – regardless of its \textit{scope}, \textit{duration}, or \textit{intensity} – occurs between the members of the armed forces of two states.}

Although this ICRC description is intended to create a very low threshold for the application of the law of armed conflict, the test remains situational and must be applied in the context in which the use of force between members of the armed forces of two states

\textsuperscript{158} 1949 Geneva Convention No. IV Commentary, \textit{supra} note 150, at 20 (emphasis added).

\textsuperscript{159} \textit{See id.} at 17-21; HOWARD S. LEVIE, 59 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES: PRISONERS OF WAR IN INTERNATIONAL ARMED CONFLICT 14-26 (1977).
is actually used. Clearly, for example, the authorized use of force by the military police of one state on one of its military installations to apprehend a visiting member of the armed forces of another state who is intoxicated and trespassing does not create *de facto* hostilities between the two states.

The United States currently utilizes a conjunctive scope, duration, and intensity analysis in its determination of belligerent status, but that has evolved over the last fifteen years from the disjunctive threshold of the ICRC commentary on Common Article 2. On December 3, 1983, two unarmed U.S. Navy planes flying in support of the U.N. Multinational Force in Lebanon were fired upon by Syrian anti-aircraft guns and surface-to-air missiles.\(^{160}\) When the United States responded the next day with airstrikes against the Syrian positions from which anti-aircraft fire had come, U.S. Navy Lieutenant Robert O. Goodman, Jr., was shot down and held by Syria.\(^{161}\) The issue of his status as a prisoner of war under the 1949 Geneva Convention No. III was raised, and the U.S. Department of State issued the following press guidance:

> **Question** – Is the captured airman a “prisoner of war” under the Third Geneva Convention?

> **Answer** – Yes. The Third Geneva Convention accords “prisoner-of-war” status to members of the armed forces who are captured during “armed conflict” between two or more parties to the Convention. “*Armed conflict*” includes any situation in which there is hostile action between the armed forces of two parties, regardless of the duration, intensity or scope of the fighting and irrespective of whether a state of war exists between the two parties. The Third Convention also provides

\(^{160}\) 3 *Cumulative Digest of U.S. Practice in International Law: 1981-88*, at 3456 (Marian Nash (Leich) ed., 1995) [hereinafter *Cumulative Digest*].

\(^{161}\) Id.
for the prompt return of prisoners when “active hostilities” have ceased. As we have made clear, the incident which occurred between our forces and those of Syria has terminated, and we are hopeful that Syria will promptly return our airman and cooperate with the Government of Lebanon in resolving the problems of that country.  


In contrast, a situation similar to Lieutenant Goodman’s resulted in a determination ten years later that a downed pilot was not a prisoner of war, but an unlawful detainee. On October 3, 1993, U.S. Army Rangers operating in support of the expanded United Nations Operations in Somalia raided a house in Mogadishu in an attempt to arrest General Mohamed Farah Aidid for previous attacks on United Nations personnel conducting humanitarian relief operations. When the raid was over, nineteen United Nations personnel were killed, and one U.S. Army helicopter pilot, Chief Warrant Officer 3 Michael Durant, was shot down and held by Somali clansmen. The issue of his status as a prisoner of war under the 1949 Geneva Convention No. III was raised, and the United States determined that he was an unlawful detainee because the United Nations operations did not rise to the level of a de facto international armed conflict that would trigger

---

162 Id. at 3456-57 (emphasis added).

163 Id. 3457.


165 Id. at 54-55.
the *jus in bello*.\(^{166}\) Warrant Officer Durant was released on October 14, 1993.\(^{167}\)

During its ratification process of the Chemical Weapons Convention, the United States adopted its current position, which raises the threshold described by the ICRC commentary. The Chemical Weapons Convention provides that “[e]ach State Party undertakes not to use riot control agents as a method of warfare.”\(^{168}\) On April 24, 1997,\(^{169}\) the U.S. Senate conditioned its consent to the Chemical Weapons Convention on the requirement that:

(26) **RIOT CONTROL AGENTS.**

(A) **PERMITTED USES.** Prior to the deposit of the United States instrument of ratification, the President shall certify to Congress that the United States is not restricted by the Convention in its use of riot control agents, including the use against combatants who are parties to a conflict, in any of the following cases:

(i) **UNITED STATES NOT A PARTY.** The conduct of peacetime military operations within an area of ongoing armed conflict when the United States is not a party to the conflict (such as recent use of the United States Armed Forces in Somalia, Bosnia, and Rwanda).

---


\(^{168}\) Chemical Weapons Convention, supra note 11, art. 1, para. 5.

\(^{169}\) Helen Dewar, *Senate Approves Chemical Arms Pact After Clinton Pledge*, WASH. POST, Apr. 25, 1997, at 1. The treaty was approved by the Senate by a vote of 74 to 26. Id.
(ii) **CONSENSUAL PEACEKEEPING.** Consensual peacekeeping operations when the use of force is authorized by the receiving state, including operations pursuant to Chapter VI of the United Nations Charter.

(iii) **CHAPTER VII PEACEKEEPING.** Peacekeeping operations when force is authorized by the Security Council under Chapter VII of the United Nations Charter.\(^{170}\)

In response, the President’s certification of April 25, 1997 provided that:

> In accordance with Condition (26) on Riot Control Agents, I have certified that the United States is not restricted by the Convention in its use of riot control agents in various peacetime and peacekeeping operations. These are situations in which the United States is not engaged in a use of force of a scope, duration and intensity that would trigger the laws of war with respect to U.S. forces.\(^{171}\)

Based upon this “shared understanding” between the Senate and the President,\(^{172}\) the United States specifically adopted a

\(^{170}\) S. Exec. Res. 75, 105\(^{th}\) Cong., CONG. REC. S3378 (daily ed. Apr. 17, 1997). The Senate gave its advice and consent to the Chemical Weapons Convention subject to a total of twenty-eight conditions. *Id.* at S3373-79.


\(^{172}\) As a result of the reinterpretation controversy of the *Treaty on the Limitation of Anti-Ballistic Missile Systems* in the early seventies, a controversial
scope, duration, and intensity analysis to determine when *de facto* hostilities exist.

This United States position is an example of the evolution of state practice that reflects the contemporary difficulty of a factual determination for *de facto* hostilities that arises because military forces are authorized to use force in self-defense\(^{173}\) and to accomplish their mission during the conduct of peacetime military operations\(^{174}\) that may occur in an area of ongoing hostilities.\(^{175}\) These peacetime military operations include law enforcement, peace-keeping, humanitarian and disaster relief, counter-terrorist, hostage rescue, and noncombatant evacuation operations.\(^{176}\) A rote constitutional principle was asserted by the Senate, and subsequently agreed upon by the Executive Branch, that “the meaning [of a treaty] is to be determined in light of what the Senate understands the treaty to mean when it gives its advice and consent.” *National Security Law* (Dycus et al.), *supra* note 60, at 194-196. Although a considerable debate continues as to the breadth of the binding effect of this principle, see *id.* at 195-98, the Executive Branch acknowledged and was very aware of the binding effect of a “shared understanding” that would be created by its communications with the Senate during the ratification process of the Chemical Weapons Convention.

\(^{173}\) See *U.N. Charter* art. 51.


\(^{175}\) Although cast as a contemporary issue, the international community was also concerned in the early 1960s over the possibility that the United Nations peace-keeping forces in the Congo may have become involved in hostilities that invoked the *jus in bello*. FINN SEYERSTED, UNITED NATIONS FORCES IN THE LAW OF PEACE AND WAR 60, 180 (1966).

application of the Common Article 2 threshold allows a limited and intermittent use of force to invoke a state of *de facto* hostilities and unintentionally causes military personnel to become belligerents and lawful targets even though they are conducting a peacetime military operation. State practice has demonstrated this rote application of international law to be politically unacceptable to the international community.177

As a result of this unintended consequence when the Common Article 2 threshold is applied to peacetime military operations, particularly those under the authority of the United Nations, the international community has rejected the disjunctive threshold of the ICRC Commentary as too restrictive. For example, one scholar concludes that an armed attack occurs, and thus an armed conflict exists, “when force is used on a relatively large scale and with substantial effect.”178 Another scholar concludes that a use of force must reach a certain “gravity” as a matter of law, and that minor frontier incidents are not *per se* a use of force that rises to the Article 2(4) threshold because “the minor nature of an attack is prima facie evidence of absence of intention to attack, of honest mistake, or simply the limited objectives of an attack.”179

The international community now subjectively analyzes the use of force by an independent state, and whether such force constitutes an armed attack, in the context of its scope, duration, and intensity. Accordingly, *de facto* hostilities exist between two

177 For a more detailed examination of this state practice, see Sharp, *supra* note 174, at 93-183.


179 *See BROWNLIE, supra* note 89, at 366.
states when the scope, duration, and intensity of force between them reaches the level of an armed attack within the meaning of Article 51 of the Charter. The conjunctive threshold does not add much more clarity to what precise level or quantum of force is required to trigger the Common Article 2 threshold. In practice, however, the application of the conjunctive test recognizes a more reasoned balancing of all of the circumstances surrounding the use of force.

Conclusion

Figure 2 graphically summarizes these principles of existing international law. It depicts the line of belligerency as that point on the use of force spectrum at which international armed conflicts begin and the law of armed conflict applies. This point is triggered by the declaration of war, the occurrence of de facto hostilities, and all cases of partial or total occupation. De facto hostilities exist when the use of force between two states reaches the scope, duration, and intensity that state practice defines as an armed attack. The law of conflict management applies during peacetime and armed conflict, and the obligations of the parties to an armed conflict under the peacetime regime of international law remain in place to the extent they are not inconsistent with a state of hostilities. Accordingly, the line which represents the application of the peacetime regime during armed conflict is dotted.
Part II: The Law of Conflict Management – The Legacy of War

The Application of International Law

© 1997 Walter Gary Sharp, Sr.

Figure 2

Information Operations

Line of belligerency

Peacetime military operations
- law enforcement
- normal peace-keeping
- humanitarian & disaster relief
- counter-terrorist & hostage rescue
- noncombatant rescue

Self-defense

Limited use of force

Use of Force Spectrum

jus ad bellum applies

jus in bello applies

Combatant operations
- declared war
- de facto hostilities
  (scope, duration, & intensity)
- partial or total occupation

All necessary means in response to outright aggression

Peacetime regime applies
In summary, short of an actual declaration of war or a case of partial or total occupation, a state does not become a party to an international armed conflict until such time as it becomes engaged in a use of force of a scope, duration, and intensity with another state that reaches the level of an armed attack within the meaning of Article 51 of the Charter. What constitutes a use of force of a scope, duration, and intensity that constitutes an armed attack and triggers the law of armed conflict is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances.

This question of fact also defies rote, categorical definition. For example, military forces conducting a noncombatant evacuation operation do not become a party to an armed conflict when they use limited force to rescue personnel. Similarly, military forces serving under the authority of the United Nations do not become a party to an armed conflict when they use limited force to accomplish an assigned humanitarian relief or peace operation. In contrast, individual or collective military action in response to outright aggression, such as the coalition response to the Iraqi aggression that led to the Persian Gulf war, does cross the Common Article 2 threshold and trigger the application of the jus in bello. This chapter was intended to provide a historical context and an understanding of the basic principles surrounding the Common Article 2 threshold and the interrelationship between an armed attack and armed conflict. A detailed analysis of how this threshold specifically applies in CyberSpace is provided in Chapter 6, infra.
Chapter 5: Delineating the Rules

Sources of international law

The general rule of international law and sovereignty is that states are only bound by those rules of international law to which they themselves have agreed.\textsuperscript{180} Even the coercive authority of the Security Council is based upon the Member States’ agreement that it has the authority to direct nonconsensual, binding measures in matters of international peace and security.\textsuperscript{181} This general principle is limited only to the extent that state practice develops into customary international law, which is binding on all states.\textsuperscript{182}

Article 38(1) of the Statute of the International Court of Justice, one of the six principal organs of the United Nations, requires the Court to apply

a. \textit{international conventions}, whether general or particular, establishing rules expressly recognized by the contesting states;

b. \textit{international custom}, as evidence of a general practice accepted as law;

c. the \textit{general principles of law} recognized by civilized nations;

d. subject to the provisions of Article 59, \textit{judicial decisions} and the \textit{teachings of the most highly qualified publicists} of the

\textsuperscript{180} \textit{The Charter of the United Nations: A Commentary, supra} note 68, at 83.

\textsuperscript{181} See \textit{U.N. Charter} arts. 25, 39-42, 48-49.

\textsuperscript{182} \textit{The Charter of the United Nations: A Commentary, supra} note 68, at 83. Customary international law results from a general and consistent practice of states followed by them out of a sense of obligation. This creates an interesting cycle of policy decisions that create precedent which in turn influences policy and creates customary international law over time.
various nations, as subsidiary means for the determination of rules of law. 183

This article is recognized as the most authoritative description of the sources of international law.

The first three categories of Article 38(1) are not listed in an order of legal hierarchy which mandates the application of one over the other, 184 but generally speaking, international conventions may be more specific and on point in a given interstate controversy than international custom. Similarly, international custom may be more relevant to an interstate dispute than general principles of national law. The unique nature of a dispute between two contiguous states, however, may make the general principles of the national law of the parties not only more relevant, but controlling. The final category of Article 38(1) considers the judicial decisions and the teachings of the most highly qualified publicists of various nations as a subsidiary means for the determination of the rules of international law. These decisions and teachings “are considered to be indicative of the interpretation and application” of international law. 185

183 Statute of the International Court of Justice, art. 38(1) [hereinafter Statute of the ICJ] (emphasis added). The Statute was adopted in 1945 as an annex to the Charter. See U.N. Charter art. 92. All Member States are parties to the Statute of the ICJ by operation of art. 93 of the Charter. Only states may be parties in cases before the ICJ. Statute of the ICJ, art. 34. Article 59 of the Statute of the ICJ provides that the decision of the ICJ has “no binding force except between the parties and in respect of that particular case,” i.e., the principle of stare decisis does not apply to decisions of the ICJ.


185 Id.
Reliance upon state practice

No international convention, to include the Charter of the United Nations, defines “threat or use of force,” “armed force,” or “armed attack,”186 and despite decades of earnest work, the international community has failed to define aggression with any clarity in any other document.187 Existing international law that governs the use of force must therefore be derived from a heuristic analysis of how the Charter use of force paradigm has been interpreted through state practice. Based upon this study of state practice, and how it is interpreted by highly qualified publicists, a profile of what is acknowledged by the international community as a use of force can be derived by studying the legal justifications and conclusions states make with regard to their activities.

States may often explicitly acknowledge what they consider a use of force, for example, when they declare the lawfulness of their activities in terms of the Charter’s conflict management paradigm. For example, the United States justified the lawfulness of its August 1998 missile strikes against terrorist camps in Afghanistan and Sudan as an exercise of its right to self-defense as recognized by Article 51 of the Charter.188 Chapter 3, supra, concluded that what constitutes a prohibited “threat or use of force” is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and

186 Id. 111-12.

187 See generally, e.g., THOMAS AND THOMAS, supra note 85.

circumstances. A questioned state activity that is considered a use of force within the meaning of Article 2 is unlawful under international law unless it is

- an exercise of that state’s right of individual or collective self-defense as authorized by international law and recognized by Article 51 of the Charter, or
- authorized by the Security Council acting under its Chapter VII coercive authority,

regardless of whether the activity occurred partially or completely in the physical world or CyberSpace. Chapter 3 also concluded that a state never loses its right to use force in self-defense in response to a use of force within the meaning of Article 2(4), however, the right of self-defense under customary international law may not justify an armed response.

At other times, states may implicitly acknowledge what they consider a use of force when they declare the lawfulness of their activities by asserting conclusions, such as whether their activities have resulted in an international armed conflict or whether the law of armed conflict applies. From these conclusions, we can determine what states consider a use of force because a questioned state activity that has been generally accepted by the international community as having created the legal status of an international armed conflict or as having invoked the law of armed conflict, is for that reason considered a use of force prohibited by Article 2(4) of the Charter. The most obvious example that clearly supports this proposition is the 1990 Iraqi invasion of Kuwait. Not only did the international community immediately declare the invasion to be an unlawful use of force, it also concluded that Iraq’s use of force invoked the legal status of an international armed conflict and the law of armed conflict. Chapter 4, supra, concluded that what constitutes a use of force of a scope, duration, and intensity that triggers the law of
armed conflict is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances.

The precise converse of this last proposition is not true under all circumstances for two reasons. First, those state activities which do not invoke the law of armed conflict obviously include noncoercive activities such as those inherent in normal diplomatic relations. Second, since international law evolves through state practice, which is motivated principally by political considerations and national interests, the converse proposition may simply be politically unacceptable and rejected by United Nations and state practice. Accordingly, a questioned state activity which has been generally accepted by the international community as not having created the legal status of an international armed conflict or as not having invoked the law of armed conflict, will usually, but not always, be considered below the use of force threshold prohibited by Article 2(4).

For example, when Chief Warrant Officer 3 Michael Durant was shot down in October 1993 during a raid on General Aidid’s stronghold and held by Somali clansmen, the United States asserted that he was an unlawful detainee and not a prisoner of war because the United Nations operations did not rise to the level of a de facto international armed conflict that would trigger the jus in bello. It was politically unacceptable for the United

---


191 See Lepper, supra note 166, at 359, 362-64.
States and the international community to characterize these forces as combatants during an international armed conflict, notwithstanding specific Security Council Chapter VII approval to use armed military force to arrest General Aidid.\footnote{Although this raid serves as a useful example, this is obviously an over simplification of the legal analysis. One very important factor to consider is the fact that it was very debatable that General Aidid and his forces represented any thing other than an armed criminal band of thieves and not the organized military of another state. It was also very important to the conclusion above that the raid was authorized by the coercive authority of the Security Council as a use of force that served to protect peacekeepers and other civilians during United Nations humanitarian operations in Somalia. For an excellent review of the United Nations operations in Somalia and a comprehensive collection of almost all of the relevant documents, see The United Nations and Somalia: 1992-1996, supra note 164.}

Similarly, consider the case of noncombatant evacuation operations that do not invoke the \textit{jus in bello} but nevertheless are considered a use of force. Later in this text, Chapter 6 concludes that international law considers such a rescue of nationals a use of force within the meaning of Article 2(4), but, as previously discussed in Chapter 4, international law does not consider such activity to be of the scope, duration, and intensity that invokes an international armed conflict. In summary, a \textbf{use of force within the meaning of Article 2(4) will always invoke a victim state’s right of self-defense, but it may not always rise to the scope, duration, and intensity threshold of an armed attack that invokes a \textit{de facto} international armed conflict and the \textit{jus in bello}.} This is consistent with the universally accepted view that the thresholds of Articles 2(4) and 51 are different in scope; \textit{i.e.}, the Article 2(4) concept of a ‘threat or use of force’ is much broader than the Article 51 threshold of ‘armed attack.’\footnote{See The Charter of the United Nations: A Commentary, supra note 68, at 663.}
Conclusion

There are significant similarities between the Article 2(4), Article 51, and the Common Article 2 thresholds, however, it should be reemphasized at this point that there is but one conflict management paradigm, and that is found in the Charter of the United Nations. The Common Article 2 threshold of the four Geneva Conventions of 1949 is not a separate paradigm of conflict management. A study of state practice and the writings of publicists, jurists, and scholars that interprets Common Article 2 simply helps define what quantum of force is necessary to rise to the level of the Article 2(4) and Article 51 thresholds.

Since there is no accepted norm within the international community that defines what is a lawful or unlawful use of force, it is helpful as state practice is reviewed to map it out in a linear model of interstate activities by building upon Figure 1. Figure 3 continues this development of a linear model for a heuristic use of force analysis by adding the Common Article 2 analysis discussed in Chapter 4 and this chapter to Figure 1. This will provide a profile of what will likely be considered by the international community to be use of force in CyberSpace.

The outer limits of this model can be plotted by starting with the polar extremes that are universally accepted examples of what does and does not constitute a use of force and an armed attack. For example, the left end should begin with full diplomatic and consular relations, because they are accepted as the desired status quo between two states and do not constitute a use of force. Similarly, states agree that a unilateral decision by a state not to trade with another is not a use of force, regardless of the potential impact of that trade decision. This end of the spectrum represents those activities that do not rise to the level of a scope, duration, and intensity that either constitutes a use of force or an armed attack.
Part II: The Law of Conflict Management – The Legacy of War

The rules defining the use of force

© 1998 Walter Gary Sharp, Sr.

Figure 3

The Spectrum of Interstate Relations

Activity Threshold

- Normal diplomatic & consular relations;
- Trade decisions.

Activity

Line of belligerency

- Declared war;
- de facto hostilities;
- Partial or total occupation.

Spectrum of Interstate Relations

- Art. 39
  - Threat to the peace
- Art. 2(4)
  - Threat of force
- Art. 51
  - Armed attack (use of force)
Chapter 5: Delineating the Rules

Self-defense

Art. 2(4)

Art. 39

Anticipatory self-defense

UNSC may require states to comply with Art. 41 measures by the UNSC under Chapter VII

Any measures or use of force authorized

Diplomatic measures; severance of diplomatic relations; complete or partial interruption of economic relations or interstate communications; arbitration, judicial proceedings, etc.

Art. 51

Responde

jus in bello applies

peacetime regime applies

jus ad bellum applies
At the other extreme, the model should end on the right side with the three factual conditions of the Common Article 2 threshold for when an international armed conflict exists. This end of the spectrum represents those activities that do clearly rise to the level of a scope, duration, and intensity that constitutes a use of force and an armed attack. What remains between these polar extremes will be profiled in the next chapter with a study of state practice.
Part III: State Activities in CyberSpace –
Defining What is a Use of Force and an Armed Attack

Chapter 6: Application of Existing Rules

Introduction

The Preamble of the Charter of the United Nations provides that one of its four goals is to ensure “that armed force shall not be used, save in the common interest . . .” \(^{194}\) To further this goal, all Member States agreed in Article 2(3) that they “shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.” \(^{195}\) The Charter provides for a number of institutional arrangements to settle disputes such as

- granting authority to the General Assembly to discuss any issue that relates to international peace and security or the welfare of the international community,
- a strong role for the Security Council in dispute settlement,
- coercive authority of the Security Council when international peace and security is threatened, and
- the International Court of Justice. \(^{196}\)

---

\(^{194}\) U.N. CHARTER pmbl.

\(^{195}\) U.N. CHARTER art. 2(3).

\(^{196}\) See THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 99.
Part III: State Activities in CyberSpace – Defining Use of Force and Armed Attack

Article 2(3) is a legally binding waiver of the sovereign right of Member States\textsuperscript{197} under international law to aggressively use force, and they agreed to enforce their obligation to settle their disputes peacefully with the prohibition on the aggressive use of force found in Article 2(4).

Modern international relations, however, is based on a sovereign nation-state system and is “motivated by national interest as its ultimate purpose.”\textsuperscript{198} These national interests, and the perceived national interests, of some 180 or more nation-states seem to cause interstate disputes and tensions to remain as a constant in the midst of countless diverse cultures, religions, and ideologies. An effective foreign policy takes into account these varying national interests, and “[d]iplomacy has many peaceful ways for bringing influence to bear” to resolve disputes.\textsuperscript{199}

While the phrase “use of force” is commonly understood to include a military attack of one state by the organized military of another state, \textit{i.e.}, an armed attack, \textbf{some coercive state activities that fall short of an armed attack may also cross the thresholds of Article 2}.\textsuperscript{200} The phrase “use of force” also applies to all agencies and agents of a state government, such as the organized military, militia, security forces, police forces, intelligence

\textsuperscript{197} The term “Member States” refers to states that are members of the United Nations and therefore a party to the Charter of the United Nations. The International Court of Justice explicitly held in its \textit{Nicaragua} judgment of June 27, 1986 that the obligation under Article 2(3) is also customary international law. \textit{THE CHARTER OF THE UNITED NATIONS: A COMMENTARY}, \textit{supra} note 68, at 100.

\textsuperscript{198} \textit{HENRY KISSINGER, DIPLOMACY} 17 (1994).

\textsuperscript{199} \textit{EUGENE V. ROSTOW, TOWARD MANAGED PEACE} 22 (1993).

\textsuperscript{200} \textit{BROWNLEI, supra} note 89, at 361-2.
personnel, mercenaries, and other surrogate forces or volunteers.201 Defining what constitutes a use of force in a full spectrum of potential state activity requires a thorough understanding of how Article 2 has been interpreted under international law. This chapter will explore state practice and the writings of jurists to develop an understanding of the Article 2(3) obligation as well as the Article 2(4) prohibition, and will then apply each of those discussions to state activities in CyberSpace.

**Obligation to settle by peaceful means**

A majority of writers suggest that “states are under an obligation to deploy active efforts for the settlement of their international disputes.”202 Accordingly, those actions must be conducted “in good faith and in a spirit of co-operation.”203 Article 2 does not mandate a specific result, only that the parties strive in good faith for the resolution of a dispute.204 It is recognized that even with good will on both sides, some disputes cannot be resolved by the parties involved in the dispute.205 Parties are expected to compromise and seek a common denominator in their

---

201 *Id.* at 361.

202 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 101. A dispute arises when one state rejects a specific claim of another state; *i.e.*, this article does not impose upon states a legal obligation to live together “in full harmony and without any political antagonism.” *Id.* at 102.

203 *Id.* at 101.

204 *Id.*

205 *Id.*
negotiations, but they are not required to behave in a manner that adversely affects their rights on balance.206

If the parties are unable to reach a resolution on their own, the General Assembly has the authority to make recommendations in the form of non-binding resolutions.207 Similarly, in matters which are “likely to endanger the maintenance of international peace and security,” the Security Council has the authority under Chapter VI of the Charter to investigate and make non-binding recommendations.208 When the dispute becomes a threat to the peace or results in either a breach of the peace or an act of aggression, the Security Council has the obligation to make recommendations or decide what measures shall be taken by states to maintain or restore international peace and security.209

Peaceful means include seeking a solution by “negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, [and] resort to regional agencies or arrangements ….”210 States have a sovereign right for other states not to intervene in matters that are essentially within their domestic jurisdiction,211 and any activity that infringes upon that prohibition on intervention is not

---

206 See id. at 101-03.

207 U.N. CHARTER arts. 14, 35.

208 See generally U.N. CHARTER chap. VI.

209 U.N. CHARTER art. 39.

210 U.N. CHARTER art. 33.

211 U.N. CHARTER art. 2(1) and (7).
Chapter 6: Application of Existing Rules

peaceful within the meaning of Article 2(3).212 An exception applies to a state’s obligation to settle their disputes exclusively by peaceful means when the dispute has been triggered by an unlawful act of one of the parties involved.213 In such cases, the aggrieved state’s right to react is extended to permit retortion and reprisal.214

If Article 2(3) requires states to actively utilize peaceful means in good faith to settle their disputes, then it prohibits states from persistently refusing “even to attempt to reach a settlement,”215 participating in activities that further threaten international peace and security by jeopardizing the resolution of its dispute, and negotiating in bad faith. Similarly, it prohibits states from interfering in other states’ disputes in such a manner that would delay settlement or otherwise threaten international peace and security. Finally, all articles must be interpreted in


213 Id.

214 Id. Retortion “connotes measures which do not infringe upon any rights of the affected state, thus constituting simple unfriendly acts.” Id. Generally, retortion refers to when a state unlawfully subjects citizens of another state to severe and stringent regulations or harsh treatment in response to similar unlawful mistreatment of its own citizens. See Black’s Law Dictionary, supra note 15, at 1183. A reprisal “is an act which is unlawful per se, unless it can be justified as a counter-measure triggered by an unlawful act and is designed to induce the offending state to return to full compliance with the law.” Id. at 105. It should be emphasized that this right of reprisal no longer includes the right to unlawfully use force contrary to Article 2(4) of the Charter. A use of force within the meaning of Article 2(4) is unlawful unless it is justified by a state’s right of self-defense or authorized by the Security Council under its coercive Chapter VII powers.

conjunction with the purposes of the Charter found in Article 1. Accordingly, any state activity which creates a dispute between two or more states would violate the Article 2(3) proscription.

Since these prohibitions apply to all potential state activities, any state activity in CyberSpace that

- is an act of bad faith as it pertains to that state’s dispute settlement negotiations,
- otherwise threatens a peaceful settlement of that state’s own dispute,
- interferes with a dispute of other states in such a manner that would delay or prevent their dispute settlement, or
- creates a dispute between other states that threatens international peace and security,

violates a Member State’s obligations under Article 2(3). For example, it would violate Article 2(3) for a state to falsify one of its own computer databases and then ‘allow’ another state access to it via the Internet in an effort to disrupt the dispute settlement negotiations. It would also violate Article 2(3) for a state to falsify one of its own computer databases and then ‘allow’ another state or states access to it via the Internet in an effort to create a dispute between two or more states. This norm does not prohibit all forms of deception between states. During peacetime, only those forms of deception that specifically violates the obligations of Article 2(3) are unlawful under the law of conflict management. During

---

216 U.N. CHARTER art. 2 provides that “[t]he Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.” See also THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 50.
armed conflict, deception is specifically permitted and governed by the law of armed conflict.

While these two hypothetical uses of the Internet and CyberSpace may violate a state’s obligations under Article 2(3), they would not be a use of force under international law. If these hypothetical uses also caused, for example, physical destruction in another state, then all the factors taken together may constitute a use of force under international law. Physical destruction and other factors that may cause a state activity to become a use of force are discussed below. In sum, what is accepted as a peaceful means under Article 2(3) is not, ab initio, a use of force within the meaning of Article 2(4). The converse is not necessarily true, i.e., a violation of a state’s obligations under Article 2(3) is not per se a use of force.

Even if not a use of force, state activities that violate Article 2(3) may nevertheless carry with them adverse consequences. Accusations of illegality, or even impropriety, may cause a state to lose political support internationally or domestically, thereby undermining the strength of a state’s negotiating position or jeopardizing a more favorable result. It may also divert attention from the actual dispute to a more collateral matter, and thereby serve the strategic advantage of an opposing state.217

217 Among the many examples that can be given in support of this conclusion, consider the recent controversy over whether the U.N. Special Commission is using its good offices to conduct intelligence operations for the United States. Regardless of the truth or accuracy of these reports, the media and public focus is now on these allegations, drawing attention from much more serious violations of international law involving the manufacture and possession of chemical and biological weapons. Fueling the debate is a discussion of the purposes and principles of the United Nations that are similar to those couched in Article 2(3). For more details of this controversy, see Barton Gellman, Annan Suspicious of UNSCOM Role, WASH. POST, Jan. 6, 1999, at 1.
Political and economic force

The scope of the Article 2(4) prohibition of the use of force is subject to dispute. The prevailing view, according to one authoritative text, is that Article 2(4) does not prohibit "any possible kind of force, but is … limited to armed force."\(^\text{218}\) Political and economic coercion may be a lawful and "permissible means of exerting pressure on other states that violate international law."\(^\text{219}\) Whether or not political and economic coercion is lawful depends upon an evaluation of the "means and ends of the measure … in relation to one another."\(^\text{220}\) This view holds that political and economic coercion may be unlawful and may be a use of force, but it is simply not a use of force prohibited by Article 2(4).\(^\text{221}\) One scholar concludes that "whilst it is correct to assume that paragraph 4 applies to force other than armed force, it is very doubtful if it applies to economic measures of a coercive nature."\(^\text{222}\)

Most of the developing countries and the former Eastern bloc countries, however, have repeatedly claimed that Article 2(4) also prohibits political and economic coercion.\(^\text{223}\) Perhaps the

\(^{218}\) The Charter of the United Nations: A Commentary, supra note 68, at 112.

\(^{219}\) Id.

\(^{220}\) Id. at 113.

\(^{221}\) Id. at 112-13.

\(^{222}\) Brownlie, supra note 89, at 362.

strongest argument in favor of the prevailing view is that the drafters of the Charter were concerned only with the use of military force, and that they explicitly rejected a proposal to extend the prohibitions of Article 2(4) to economic coercion.\footnote{Id.} Other scholars, however, have also reviewed the working documents of the drafters of the Charter, and concluded that they “do not indicate that the phrase [‘use of force’] applied only to armed force ….”\footnote{See BROWNLIE, supra note 89, at 361-2.}

The prevailing view also finds contextual support in the preamble, which provides that a goal of the Charter is to ensure “armed force shall not be used except in the common interest.”\footnote{THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 112.} Accordingly, Article 2(4) must prohibit only the use of armed force.\footnote{Id.} This argument, and the prevailing view defined by one scholar, is not persuasive because it focuses on only one goal and ignores the broader context of the Charter.

When the drafters considered the proposal to extend the prohibitions of Article 2(4) to economic coercion they could have easily used the term armed force. Instead, they chose to use only the phrase “threat or use of force” while at the same time using the term armed force more than once elsewhere in the Charter. More importantly, the preamble and the purposes of Article 1 describe a Charter that is concerned with far more than simply the use of armed force. The Charter is concerned with human rights, social progress, justice, standards of life, tolerance, and living together in
peace as good neighbors. In light of these goals and purposes, consider the final clause of Article 2(4):

   (4) All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.  
   (emphasis added)

A more balanced, contextual interpretation of Article 2(4) concludes that political and economic sanctions may indeed be a source of threats to international peace and security and an unlawful use of force that can threaten the territorial integrity and political independence of a state in violation of Article 2(4).\(^\text{228}\)

One scholar concludes, for example, that the prohibition in Article 2(4) may be violated when a state undertakes to use its political and economic power with such sufficient intensity it poses a genuine threat to the sovereignty of the target state.\(^\text{229}\) This is consistent with the conclusion of two other scholars that “[e]conomic aggression can be used as a tool to subjugate one nation to the will of another.”\(^\text{230}\) There is obviously a difference in scale and effect of a simple economic policy of a state, or a cartel of states, that defines national economic interests, and those organized policies which are intended to reach a magnitude that interferes with the political independence and territorial integrity of a state. Two scholars define this difference as follows:

\(^{228}\) See \textit{The International Legal System} 1296-97 (Joseph Modeste Sweeney et al. eds., 1981).

\(^{229}\) \textit{Id.} at 1297.

\(^{230}\) \textit{Thomas and Thomas, supra} note 85, at 90.
Although a state at international law may chart its own economic course in its relations with other states, still all states are restricted by the rule that a policy cannot be exercised for the sole purpose of causing injury to and forcing the will of another state unless such economic coercion is used in the exercise of the right of self-defense or reprisal. An illegal intervention of an economic nature becomes aggression if it jeopardizes essential rights of a state which are requisite to its security.\footnote{Id. at 90-91 (footnotes in original text are omitted).}

Accordingly, a complete contextual analysis reveals that Article 2(4) is a prohibition on a spectrum of force that does not include coercive political and economic sanctions that are intended to influence another state’s policy or actions, but ranges from state activities that begin with coercive political and economic sanctions that threaten the territorial integrity or political independence of another state to that of armed force. Boycotts, the severance of diplomatic relations, the interruption of communications, and economic competition or sanctions between states are lawful and not considered a threat or use of force. In contrast, political or economic aggression is a use of force within the meaning of Article 2(4).

Consider the application of Article 2(4)’s prohibition in CyberSpace.\footnote{While real-world conflicts are a superb way to demonstrate these principles in practice, and are used where possible in this chapter, there are no reported information operations in CyberSpace that will exemplify these principles. Accordingly, somewhat simplified hypothetical scenarios will be used to demonstrate how these principles of \textit{jus ad bellum} may restrict state activities in CyberSpace.} State A is a fifth the size of State B and, except for one very small border along a lake, is geographically an enclave of State B. State A, apparently based upon insider information internal to State B, has been subsidizing its currency on the global
market in such a way that it devalues the currency of State B. This is the deliberate intent of State A because its President dislikes a number of the economic policies of State B. The devaluation is not significant, but it does adversely effect the trade balance of State B.

In response, State B restricts its national companies from broadcasting any economic or financial news into State A. Such a political and economic policy, or ‘sanction,’ is a lawful response to State A’s financial policy, however, it is unsuccessful because State A can easily get the same information from CNN.

State B then decides to further restrict the flow of information by actively jamming all CNN broadcasts that flow into State A. Assume that this expanded policy violates existing telecommunications agreements and State B’s contractual arrangements with CNN, it is therefore an unlawful act under international law, but it is not a use of force within the meaning of Article 2(4). It is also not successful. State B now creates a false database and ‘allows’ State A to hack into it, hoping to mislead State A and undermine its ability to devalue the currency of State B. Similarly, this information operation by State B is not a use of force, and is unsuccessful.

In frustration, State B completely jams all electronic transmissions into, out of, and within State A. This has a devastating effect on State A. All telecommunications within and by State A with other states have ceased. Emergency services are significantly curtailed throughout State A, and the flow of emergency medical data between hospitals has stopped. No financial transaction can occur electronically within State A or between anyone in State A and someone in another state. The volume of imports and exports have dropped sharply by 95% from the previous month. State A cannot communicate electronically with its embassies around the world, regional organizations, or the
United Nations. Without a single shot being fired, State A has effectively been brought to its knees in a few short months and is at the complete mercy of State B. To survive, State A must surrender to the will of State B. State B’s virtual blockade of State A is a use of force within the meaning of Article 2(4). Indeed, it is the electronic equivalent of an armed attack, and is unlawful under these circumstances because it was not justified by any right of self-defense.

**Threats of the use of force**

A threat of force “consists in an express or implied promise by a government of a resort to force conditional on non-acceptance of certain demands of that government.”\(^{233}\) State practice has demonstrated a “relatively high degree” of tolerance towards mere threats to use force because most were in the context of self-defense.\(^{234}\) A threat to use force is unlawful if not made under conditions that otherwise make the actual use of force lawful.\(^{235}\) For example, it is unlawful under Article 2(4) for a state to make “a blatant and direct threat of force, used to compel another State to yield territory or to make substantial political concessions . . . ”.\(^{236}\)

\(^{233}\) Brownlie, supra note 89, at 364.

\(^{234}\) The Charter of the United Nations: A Commentary, supra note 68, at 118.

\(^{235}\) Brownlie, supra note 89, at 364; The Charter of the United Nations: A Commentary, supra note 68, at 118.

\(^{236}\) The Charter of the United Nations: A Commentary, supra note 68, at 118.
This principle does place restrictions on state activities in CyberSpace. Isolated threats are usually verbal in nature and do not implicate the use of CyberSpace except as a transmission medium for the threat. To the extent, however, that unlawful verbal threats are reinforced or conveyed by state activities in CyberSpace, those activities may become an integral part of the unlawful threat and thus become an unlawful use of force.

State activities that constitute a threat or cause the perception of a threat create special problems in conflict management because they constitute circumstantial evidence of impending hostile acts and hostile intent. Threats serve to give definition to the intent of the acting state and the perceptions of a potential victim state. Hostile act and hostile intent are the operational concepts that are integral to the rules of engagement (ROE) of a state that implement its inherent right of self-defense. The “Standing Rules of Engagement for US Forces” (SROE) defines hostile act and hostile intent as follows:

e. **Hostile Act.** A hostile act is an attack or other use of force by a foreign force or terrorist unit (organization or individual) against the United States, US forces, and in certain circumstances, US citizens, their property, US commercial assets, and other designated non-US forces, foreign nationals and their property. It is also force used directly to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel and vital US Government property. When a hostile act is in progress, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. …

f. **Hostile Intent.** Hostile intent is the threat of imminent use of force by a foreign force or terrorist unit (organization or individual) against the United States, US forces, and in certain circumstances, US citizens, their property, US commercial assets, or other designated non-US forces, foreign nationals and their
property. When hostile intent is present, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. …

Isolated verbal threats, and threats of the use of force that are conveyed by initial troop movements, the shaping of alliances, or initial Intermediate Range Ballistic Missile (IRBM) movements, likely do not constitute hostile intent. Threats of the use of force conveyed by the massing of troops or IRBMs on the border, the tactical use of fire control radar, and the interference with early warning (EW) or command and control systems, are very likely to be considered an indication of hostile intent. **State activities that convey hostile intent constitute a threat to use force, and a state which is the object of that hostile intent has the right to use necessary and proportional force to respond in anticipatory self-defense.**

In comparison, hostile acts include blockades; the destruction of early warning or command and control systems; and those uses of force against the territory, warships, military aircraft, military forces, or the citizens of a state abroad. **Although all uses of force are not of the scope, duration, and intensity to constitute an armed attack, state activities that constitute a hostile act are a use of force that constitutes an armed attack, and a state which is the object of that hostile act has the right to use necessary and proportional force to respond in self-defense.**

---

Consider the situation that is clearly an unlawful threat of the use of force. Before the virtual blockade, State B threatens to use armed military force to invade and occupy State A if it does not immediately cease subsidizing its currency to the detriment of State B. Since the devaluation is not significant, State B does not have the right to threaten or use force in self-defense.

State A scoffs at the threat. To reinforce the seriousness of its unlawful threat, State B proves how easily it can control an occupied State A by jamming CNN and all international telecommunications that flow into State A for five minutes every hour on the hour. In the previous discussion on political and economic force, it was assumed that the jamming of telecommunications that flow into State A was unlawful under existing telecommunications agreements and other contractual obligations of State B, but that such unlawful jamming was not a use of force within the meaning of Article 2(4). Similarly, the unlawful jamming of all incoming telecommunications in this situation is not a use of force within the meaning of Article 2(4) or an armed attack, but, as an extension of the unlawful verbal threat to use force, it is an unlawful threat to use force within the meaning of Article 2(4).

Since the jamming activities of State B are only a threat to use force, State A does not have the right to use force in self-defense. This hypothetical, however, is an example of the special problems of conflict management caused by threats and the perceptions of threats that demonstrate hostile intent. In the context of State B’s threats to use armed military force to invade and occupy State A, State B’s jamming of all telecommunications that flow into State A could be subjectively perceived by State A as a demonstration of hostile intent that is a prelude to the threatened invasion and occupation. Under these circumstances, State A does have the lawful right to use force in anticipatory self-defense. As concluded in Chapter 3, supra, what constitutes a
prohibited ‘threat or use of force’ is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances.

**Violations of international law**

Violations of international law are not *per se* a use of force and the unlawfulness of those violations follows from international norms other than Article 2(4).\(^{238}\) A violation of international law, however, “which involves an exercise of power in the territorial domain but no use of arms” may constitute an unlawful use of force prohibited by Article 2(4).\(^{239}\) While there appears to be no evidence in the working documents of the drafters of the Charter to support this view,\(^ {240}\) issues concerning a prohibited use of force have arisen under state practice when the territorial integrity of a state has been violated despite the fact that no armed military force occurs.

The Soviet government, for example, has asserted that military intelligence flights by reconnaissance aircraft over Soviet territory and territorial waters are *per se* acts of aggression.\(^ {241}\) The Soviet response to the 1960 U-2 flight by the United States over Soviet territory emphasizes that under modern conditions “the incursion of a single plane is ‘an act of aggression’ because it

---


240 Brownlie, supra note 89, at 362-63.

241 Id. at 363.
might carry a deadly load and, further, might cause those in charge of detection systems to order retaliation on the assumption that an attack had begun.”242 The United Nations Security Council disagreed, and concluded that the U-2 flight was a violation of Soviet airspace but not a use of force within the meaning of Article 2(4).243 Also contrary to the Soviet position, one scholar concludes that military intelligence flights and tactics of psychological warfare may be deliberate and illegal intrusions, but are not necessarily a use of force.244 The consensus view is that while all nations have complete and exclusive sovereignty over their national airspace and never lose their inherent right of self-defense, customary international law requires a reasonable response to civilian and military aircraft that violate another state’s airspace that is proportionate to the danger posed by the presence of the trespassing aircraft.245

The danger posed by the presence of a trespassing aircraft is a subjective determination that must be based upon the circumstances at the time of the actual or perceived attack.246 Intrusions into another state’s territory “may be regarded by the state which is their object as circumstantial evidence of an intention to attack or preparation for future attacks,”247 thereby

242 Id.

243 NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 439.

244 BROWNLIE, supra note 89, at 364.

245 See NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 439; COMMANDER’S HANDBOOK, supra note 107, ¶ 4.4; BROWNLIE, supra note 89, at 363-64, 373-74.

246 See generally COMMANDER’S HANDBOOK, supra note 107, ¶ 8.1.1.

247 BROWNLIE, supra note 89, at 364.
giving rise to concepts such as hostile act and hostile intent. While international law is not completely clear in these cases of trespass, the right of self-defense may be invoked when a territorial state perceives a threat or use of force and has no alternative but to act to defend itself. All of the relevant circumstances must be subjectively analyzed to determine whether a threat or use of force, or a perception thereof, has occurred.

If the trespasser, for example, is an “unidentified fast aircraft which persists in a deliberate and deep penetration of airspace, it may be that, in view of the destructive power of even a single nuclear weapon carried by an aircraft, the territorial sovereign is justified in taking without any warning violent and immediate preventive measures.” In the context of a land invasion by armed troops, one scholar concludes that an incursion into the territory of another state constitutes an infringement of Art. 2(4), even if it is not intended to deprive that state of part of its territory and if the invading troops are meant to withdraw immediately after completing a temporary and limited operation (‘in-and-out operations’). In other words, ‘integrity’ has to be read as ‘inviolability’, proscribing any kind of forcible trespassing.

In contrast, it is “very doubtful if maritime trespassers in territorial waters may be subjected to violent measures unless they are engaged in an attack or are carrying aid to rebels.”

---

248 See id.

249 See id. at 373.


251 See Brownlie, supra note 89, at 374.
guidance from the International Court of Justice is that a trespasser must “be given reasonable opportunity to leave peacefully and measures against him should be preventive and not punitive.”

Violations of international law may constitute a use of force within the meaning of Article 2(4) if they involve an exercise of power in the territorial domain of another state, even without the use of arms, but the response in self-defense must be necessary and proportional in view of the danger posed by the violation.

In the hypothetical scenario between States A and B, recall that as part of State B’s unlawful threat to invade State A before the electronic blockade, it jams CNN and all international telecommunications that flow into State A for five minutes every hour on the hour. In previous discussions, it was concluded that the jamming of telecommunications that flow into State A was not a use of force within the meaning of Article 2(4), although it was assumed that it violated telecommunications agreements and other contractual obligations of State B.

After five days of jamming external telecommunications flowing into State A, State B desires to strengthen its threat by completely jamming all electronic transmissions within, into, and out of State A for five minutes every hour on the hour. This constitutes an exercise of power in the territory of State A in violation of international law that constitutes a use of force within the meaning of Article 2(4), even in the absence of the context of the unlawful threat.

This violation of international law is a use of force, but it is not of the scope, duration, and intensity to constitute an armed attack. State A does, however, have the right of self-defense, and

---

252 See id. at 364 n.3.
it could take necessary and proportionate measures to destroy or neutralize the source of the unlawful jamming. Moreover, such jamming could be considered by State A as an indication of hostile intent, \textit{i.e.}, the beginning of an invasion by State B, thereby escalating the situation to actual hostilities if State A preemptively attacks under its right of anticipatory self-defense.

\textbf{Unarmed, non-military physical force}

Recognizing that unarmed, non-military physical force by a state can affect another state just as severely as the use of armed military force, the \textit{Article 2(4) prohibition on the use of force also covers “physical force of a non-military nature”}\textsuperscript{253} committed by any state agency.\textsuperscript{254} Examples of such unarmed physical force include “the cross-frontier expulsion of populations, the diversion of a river by an up-stream state, the release of large quantities of water down a valley, and the spreading of fire across a frontier.”\textsuperscript{255} \textit{It is also recognized that unarmed, non-military physical force “may produce the effects of an armed attack prompting the right of self-defense laid down in Art. 51.”}\textsuperscript{256}

This principle places far-reaching restrictions on a state’s activities in CyberSpace that ‘attack’ the critical infrastructure of another state and cause destructive effects. A state can potentially

\begin{itemize}
\item \textsuperscript{253} \textit{See} \textit{THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra} note 68, at 113.
\item \textsuperscript{254} \textit{BROWNLIE, supra} note 89, at 361.
\item \textsuperscript{255} \textit{THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra} note 68, at 113. \textit{See also} \textit{BROWNLIE, supra} note 89, at 362-63.
\item \textsuperscript{256} \textit{THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra} note 68, at 113.
\end{itemize}
cause significant property and economic damage, as well as human fatalities, in another state by utilizing the Internet to cause

- flooding by opening the gates of a dam,
- train wrecks by switching tracks for oncoming trains,
- plane crashes by shutting down or manipulating air traffic control systems,
- large chemical explosions and fires by readjusting the mix of volatile chemicals at an industrial complex,
- a run on the banks or a massive economic crisis by crashing national stock exchanges,

and any number of other examples that are limited only by the imagination of the state actors. **Any destructive state activity intentionally caused within the sovereign territory of another state is an unlawful use of force.** The cross-border use of weapons and bombardment of the territory of one state by another state is one of the classic cases of a use of force within the meaning of Article 2(4).257 The effect can be the same, if not more severe, as if the destruction was caused by conventional kinetic means of warfare. Accordingly, **any state activity in CyberSpace that intentionally cause any destructive effect within the sovereign territory of another state are an unlawful use of force.**

Inadvertent damage done within the sovereign territory of another state will give rise to civil liability, but will very likely not be a use of force within the meaning of Article 2(4) that invokes a state’s right to use force in self-defense. For example, consider the hypothetical of State A using CyberSpace to attack State B in such a way that utilized the telecommunications infrastructure of State C. Then assume that this destructive activity of State A inadvertently caused severe damage to the information

---

257 *See id.* at 670.
infrastructure of State C, and perhaps even significant consequent physical damage within State C. This hypothetical highlights why use of force issues must be subjectively analyzed, as previously discussed, in each and every case in the context of all relevant circumstances. While State A has caused a destructive act in State C, State A has not engaged in a use of force against State C within the meaning of Article 2(4), and State C does not have the right to use force in self-defense against State A. State A does, however, incur civil liability under international law for the damage it caused to State C.

Furthermore, even if such intentional destructive activities are an unlawful use of force that unequivocally invokes a victim state’s right of self-defense, that right of self-defense does not necessarily justify a use of force in response. Similarly, not every destructive activity of this nature will reach the “intensity that enables them to be classified as ‘armed attacks’. ”258 The scope, duration, and intensity of the force must be analyzed to determine if an armed attack has occurred. For example, it would be an unlawful use of force but most likely not an armed attack if a state uses the Internet to cause a single train crash. Furthermore, absent a continuing threat, a use of force in response would not be authorized under the victim state’s right of self-defense. In contrast, it would very likely be considered an armed attack should a state cause dozens of such incidents, or if a state caused one major incident such as the complete and long-term crash of the New York Stock Exchange. In the case of such an armed attack, a victim state would be completely justified in using force in self-defense.

258 Id.
Protection of nationals abroad

Before the Charter’s prohibition on the aggressive use of force, states and jurists universally accepted as lawful the use of force to protect the lives and property of nationals. This position was justified on the theory that nationals of a state are an extension of the state, and that the purpose of the state is the protection of its nationals. Today, there is considerable debate among jurists over whether the nonconsensual use of military force to protect nationals abroad is a use of force proscribed by Article 2(4), and if so, whether such use of force is authorized by Article 51. One author concludes that only military units sent abroad can be the targets of an armed attack, and that diplomatic missions, individual nationals, and other external positions of a state cannot be the targets of an armed attack within the meaning of Article 51 which would invoke the right of a state to use force in self-defense. The same author, however, modifies this seemingly absolute rule by noting that attacks on the “whole of the civilian marine or air fleet,” as distinct from individual vessels or aircraft, may constitute an armed attack. When applied to actual situations, this minority position is not an absolute prohibition as much as it is an evaluation of the level of the attack that has occurred and the effect it has had on the victim state.

259 BROWNLE, supra note 89, at 289.

260 Id.


262 Id. at 671.

263 Id.
State practice, however, resolves the debate in favor of the lawfulness of such rescue operations. The United States and other nations have repeatedly rescued their own nationals abroad since the Charter entered into force, and have declared that Article 2(4) “does not prohibit the use of armed force in order to rescue a state’s own nationals whose lives or health are endangered in a foreign state, provided that the latter is not able or not willing to provide the required protection.”\textsuperscript{264} Notable examples include the protective measures taken in 1960 by Belgium in the Congo, the 1964 Belgian-United States rescue operation in the Congo, the 1976 Israeli raid on Entebbe, the 1980 attempt by the United States to rescue its diplomatic staff held hostage in Iran, the 1983 rescue operation by the United States in Grenada, and the 1989 intervention in Panama by the United States to protect its nationals.\textsuperscript{265}

A growing number of noted jurists and scholars have justified the lawfulness of these military operations under one of three arguments.\textsuperscript{266} Some maintain that a use of force on such a comparatively small scale does not infringe Article 2(4) because the territorial integrity and political independence of the states concerned are not affected.\textsuperscript{267} Others recognize a case of conflicting obligations that justify these rescue operations through a weighing of protected interests.\textsuperscript{268}

\textsuperscript{264} Id. at 124.

\textsuperscript{265} Id.

\textsuperscript{266} Id. at 124-25.

\textsuperscript{267} Id. at 125.

\textsuperscript{268} Id.
The remaining and largest group of jurists conclude that the forcible protection of a state’s own nationals is lawful self-defense under Article 51.269 Their view is that if Article 51 of the Charter recognizes an inherent right of self-defense, then the content of that right must be determined by reference to customary international law.270 Before the Charter, however, international law permitted states to use aggressive force freely, and references to self-defense were politically motivated without any particular legal denotation.271 Accordingly, customary international law since the creation of the Charter’s Article 2(4) prohibition has greater value than pre-Charter customary norms.

While one scholar concludes that the “forcible protection of nationals against the will of the territorial state is illegal,”272 he acknowledges the divisiveness of the controversy among jurists. More importantly, he also concludes that state practice, supported by organs of the United Nations, demonstrates “considerable reluctance” to qualify armed rescue operations of a state’s own nationals unlawful in any case – possibly giving rise to a new customary norm.273 Another scholar concludes that three conditions for such lawful rescue operations exist in customary international law.274 Based upon the principles espoused by

269 Id. at 125 & n.156.

270 See BROWNLIE, supra note 89, at 299.


272 Id. at 125 (footnotes omitted).

273 Id. at 125-26.

274 BROWNLIE, supra note 89, at 299.
Secretary of State Daniel Webster in the *Caroline* case, he concludes that

(a) an imminent threat of injury to the nationals;
(b) a failure or inability on the part of the territorial sovereign to protect them;
(c) that the measures of protection should be strictly confined to the object of protecting them against injury.\(^{275}\)

A similar test was framed by the United States during the United Nations Security Council debate on the 1976 Entebbe incident. After reaffirming the principle of territorial sovereignty, the United States representative stated that

Israel’s action in rescuing the hostages necessarily involved a temporary breach of the territorial integrity of Uganda. Normally, such a breach would be impermissible under the Charter. However, there was a well established right to use limited force for the protection of one’s own nationals from an imminent threat of injury or death in a situation where the State in whose territory they were located was either unwilling or unable to protect them. The right, flowing from the right of self-defence, was limited to such use of force as was necessary and appropriate to protect threatened nationals from injury.\(^{276}\)

Two resolutions were presented to the Security Council after the raid on Entebbe – the United Kingdom-United States draft which condemned the hijacking in support of the Israeli rescue, and the Tanzania-Libya-Benin draft which condemned Israel’s violation of Uganda’s sovereignty and territorial integrity.\(^{277}\) Only the first was

---

\(^{275}\) *Id.*

\(^{276}\) *The International Legal System, supra* note 228, at 1287.

\(^{277}\) *Id.* at 1285-86.
brought to vote, and it failed to pass.\textsuperscript{278} In contrast to the position of the United States, the delegate from the Soviet Union stated during the Security Council debate that there are “no laws in the world, no moral or international laws, which could justify such action.”\textsuperscript{279}

The international custom of states since the creation of the Article 2(4) norm, demonstrated and reinforced by repeated state practice, is strong evidence that the nonconsensual use of limited military force that is necessary and proportional to protect nationals abroad is a use of force within the meaning of Article 2(4) and that such a use of force is lawful self-defense authorized by Article 51. Given the limited scope, duration, and intensity of nonconsensual rescue operations, they are not armed attacks. This conclusion is also supported by the writings of a growing number of scholars and jurists, which is also, \textit{ipso facto}, indicia of the existence of a customary norm.

State activities in CyberSpace would not likely constitute a rescue operation, but they very likely could be conducted in support of a rescue operation or other effort intended to protect a state’s nationals from an imminent threat of injury or harm. For example, as previously discussed, it would be an unlawful use of force for a state to shut down the air traffic control system for an entire state without justification by crashing its computers via the Internet. During a heliborne rescue operation, however, it would be a lawful act of self-defense for a rescuing state to manipulate the territorial state’s computers via the Internet to create a blind air corridor in which the territorial state is unable to detect the rescue...

\textsuperscript{278} \textit{Id.}

\textsuperscript{279} \textit{Id.} at 1288.
Chapter 6: Application of Existing Rules

aircraft. Similarly, it would be a lawful act of self-defense during a rescue operation to electronically jam anti-aircraft fire control radars either by overhead aircraft or via the Internet. It would also be a lawful act of self-defense for a state to assist its nationals, who are in imminent threat of injury or harm, to escape surreptitiously from a state by manipulating that state’s database via the Internet to falsify travel documents, identity papers, passports, or other documents or databases that would facilitate their escape.

During the nonconsensual rescue operation that is a lawful use of force in self-defense, the territorial state has the right to use force in self-defense, but that use of force must be necessary and proportional. As previously discussed in the section concerning violations of international law, all nations have complete and exclusive sovereignty over their national airspace and never lose their inherent right of self-defense. Customary international law, however, requires a reasonable response to civilian and military aircraft that violate another state’s airspace that is proportionate to the danger posed by the presence of the trespassing aircraft.280 Similarly, the International Court of Justice has held that a trespasser must “be given reasonable opportunity to leave peacefully and measures against him should be preventive and not punitive.”281 Based on these principles, if a territorial state was unaware of an ongoing rescue operation and perceived an attack on its territory, it would have the right to use armed force in self-defense to prevent the intrusion. In contrast, if circumstances were such that the territorial state was completely aware of the limited and humanitarian nature of the rescue operation, and the lack of any intent to do the territorial state any harm, its right to use

280 See COMMANDER’S HANDBOOK, supra note 107, ¶ 4.4; BROWNLIE, supra note 89, at 363-64, 373-74.

281 See BROWNLIE, supra note 89, at 364 n.3.
necessary and proportional force in self-defense would not allow the territorial state to shoot down the rescue aircraft.

**Indirect armed force**

Article 2(4)’s prohibition on the use of force also includes the use of indirect armed force and it is widely accepted that indirect force can constitute an armed attack.\(^{282}\) This Article 2(4) prohibition extends to the participation of one state in the use of force by another state, for example, “by allowing parts of its own territory to be used for violent acts against a third state.”\(^ {283}\) It also extends to a “state’s participation in the use of force by unofficial bands organized in a military manner, such as irregulars, mercenaries, or rebels.”\(^ {284}\)

The scope of this prohibition is clarified by the General Assembly’s 1970 “Declaration on Principles of International Law Concerning Friendly Relations Among States In Accordance With the Charter of the United Nations,” which provides that

> Every state has the duty to refrain from organising or encouraging the organisation of irregular forces or armed bands, including mercenaries, for incursion into the territory of another state. Every state has the duty to refrain from organising, instigating, assisting or participating in acts of civil strife or terrorist acts in another state or acquiescing in organized activities within its territory directed towards the commission of


\(^{283}\) *Id.* at 113; *Brownlie*, *supra* note 89, at 374-75.

such acts, when the acts referred to in the present paragraph involve a threat or use of force.285

Although General Assembly resolutions are not binding on states, the International Court of Justice has held that these provisions reflect customary international law.286 The prevailing view is that third states are “entitled to intervene in a civil war in support of the legitimate government, upon its request or at least with its consent, whereas giving support to rebels is said to be entirely prohibited.”287 What constitutes prohibited support remains unclear, but the International Court of Justice has held that the arming and training of irregular forces is a use of force, but not merely supplying funds.288

There are two general circumstances where this principle may restrict state activities in CyberSpace. First, and the most obvious, those state activities in CyberSpace that either support or constitute a prohibited indirect use of force are themselves unlawful as well.289 For example, it would be unlawful for one


287 Id. at 116.

288 Id. at 115.

289 This may explain why most state activities of this nature are conducted by states as covert operations which attempt to conceal the identity of the state actor.

A covert operation is so “planned and executed as to conceal the identity of or permit plausible denial by the sponsor … [which] differs from a clandestine operation in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation.” JOINT PUB 1-02, supra note 48, at 129.
state to manipulate information in another state via CyberSpace during peacetime in an effort to instigate a plot to overthrow the leader of that country. Suppose that State C wants to quietly have the president of State D overthrown. To do so, State C uses the Internet to plant rumors that the president of State D is selling the majority of the food rations purchased for his military forces for his own private gain. State C then uses the Internet to manipulate the State D’s computer databases in such a way that most of the food rations are directed ‘by the order of the President of State D’ to a local coastal port, leaving little or no food for the military forces. State C then uses the Internet to anonymously report the missing military food sitting at the port to the local press of State D. The military forces of State D are furious, and a military coup ensues. Absent the context of this occurring during an armed conflict between States C and D, State C’s activities would be an unlawful use of indirect force, but it is very unlikely it would be considered of a scope, duration, and intensity that would constitute an armed attack.

Second, it would be unlawful under customary international law for a state to allow its information infrastructure to be used by another state or insurgents to engage in violent acts against a third state. It is an unlawful use of indirect force, for example, for State E to knowingly permit or acquiesce in the use of its Internet gateways by State F during peacetime to commit unlawful uses of force against State G. Mere acquiescence would not constitute an armed attack, but using the information infrastructures to help arm or train insurgents would constitute an armed attack. If this occurs in the context of hostilities between States F and G, then State E has the duty under the law of neutrality to prevent the construction of telecommunications infrastructures by a belligerent on its territory and the use by a belligerent of telecommunications infrastructures that existed before hostilities for solely military
purposes that are not open to the public for use. As a neutral state during hostilities, State E is not obligated to forbid or restrict the use of its telecommunications infrastructure by the belligerents, but whatever restrictions are put into effect must be applied impartially to both belligerents.

**Armed attack**

Although a consensus on the meaning of armed attack is of the “utmost significance for the effectiveness of the rules of international law on war prevention,” the phrase is not defined anywhere in the Charter. It is easy, however, to identify a few state activities universally accepted as an armed attack. One scholar, for example, identifies the “Iraqi panzer blitzkrieg against Kuwait … [as] a paradigm armed attack” and concludes that if “this attack were not an armed attack … , then nothing would be.” This Iraqi attack fits squarely within the 1974 General Assembly Definition on Aggression resolution, and it was also condemned by numerous Security Council resolutions as an armed attack.

---

290 See Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, arts. 3-5, reprinted in DOCUMENTS ON THE LAWS OF WAR, supra note 2, at 63.

291 See id., at arts. 8-9.


293 MOORE, supra note 94, at 151.

294 Id. at 22-23.
Part III: State Activities in CyberSpace – Defining Use of Force and Armed Attack

While the General Assembly resolution on the Definition of Aggression\footnote{Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (1974). G.A. Res. 3314 is provided as Document G of the Document Annex.} does not define armed attack, its list of acts of aggression are considered as examples of armed attack.\footnote{THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 670.} An analysis of the Definition of Aggression resolution by one scholar that provides a widely accepted view of what constitutes an armed attack is summarized as follows:

(a) \textit{Invasion, bombardment and cross-border shooting}. These examples represent the classic cases of armed attacks, provided “that the military actions are on a certain scale and have a major effect, and are thus not to be considered mere frontier incidents.”

(b) \textit{Blockade}. An effective blocking of a state’s ports or coasts by the armed forces of another state is an armed attack. The barring of passage for land-locked states to the open sea across another state’s territory has not been accepted as an armed attack.

(c) \textit{Attack on the land, sea, or air forces or on the civilian marine and air fleets}. An armed attack occurs when the armed forces of one state attacks the land, sea, or air forces, or the civilian marine and air fleets, of another state. The regular forces of a state, wherever they are, always have the right to defend themselves by military force.

(d) \textit{Breach of stationing agreements}. An armed attack may occur when a state uses its armed forces within the territory of another state in contravention of the conditions provided for in the agreement, or any
extension of their presence beyond the termination of the agreement; provided, however, that the breach of the terms of the agreement has the effect of an invasion or occupation.

(e) *Placing territory at another state’s disposal.* The voluntary action of a state in allowing another state to use its territory for committing an armed attack is also an armed attack.

(f) *Participation in the use of force by militarily organized unofficial groups.* It is widely accepted that indirect force falls under the definition of armed attack. The sending of armed bands to use armed force in another state makes the armed bands *a de facto* state agent, thus the sending state has engaged in an armed attack. Similarly, ‘substantial involvement’ in the activities of an armed band may also constitute an armed attack.297

An armed attack may also occur when a state uses “bacteriological, biological, and chemical agents” against another state, even though they may “not involve any explosive effect with shock waves and heat.”298 Although these ‘weapons’ may be used by the military in conjunction with other traditional weapons, the use of these devices may constitute an armed attack when a state uses any of its civilian agencies to release the agents in another state.

One key point to take away from this summary is that an armed attack may occur when a use of force or an activity not traditionally considered an armed attack is used in such a way that it becomes tantamount in effect to an armed attack.

---

297 Id. at 669-74.

298 Brownlie, *supra* note 89, at 362.
Accordingly, state practice defining what is an armed attack within the meaning of Article 51 of the Charter places far-reaching restrictions on state activities in CyberSpace.

This chapter has provided a number of examples of state activities in CyberSpace that define what is and what is not an armed attack within the meaning of Article 51 of the Charter. All of these examples are consistent with the views of the scholar discussed above on the Definition of Aggression. For example, in the discussion of political and economic force, State B’s virtual blockade of State A was determined to be a use of force within the meaning of Article 2(4) and a CyberSpace equivalent of an armed attack. This is consistent with the conclusion of one scholar that in extreme cases where an impairment is equivalent to a “military invasion (e.g., by cutting off all communication routes) an ‘armed attack’ can be taken to exist.”

In the discussion of threats of the use of force, State B’s jamming of CNN and all other international telecommunications that flowed into State A for five minutes every hour on the hour, in the context of reinforcing an unlawful threat to invade, was determined to be an unlawful threat to use force within the meaning of Article 2(4). It was not, however, considered a use of force within the meaning of Article 2(4) or an armed attack.

In the discussion of violations of international law, State B strengthened its threat by completely jamming all electronic transmissions within, into, and out of State A for five minutes every hour on the hour. This constituted an exercise of power in the territory of State A in violation of international law that constituted a use of force within the meaning of Article 2(4), but

---

was not of the scope, duration, and intensity to constitute an armed attack. It was also noted that such jamming could be considered by State A as the beginning of an invasion by State B, thereby escalating the situation to actual hostilities if State A preemptively attacks under its right of anticipatory self-defense.

In the discussion of unarmed, non-military physical force, it was concluded that all state activities in CyberSpace that intentionally cause any destructive effect within the sovereign territory of another state are an unlawful use of force. It was concluded that if a state uses the Internet to cause a single train crash in another state, it would be an unlawful use of force but not one of a scope, duration, and intensity to constitute an armed attack. In contrast, it would very likely be considered an armed attack should a state cause dozens of such incidents, or if a state caused one major incident such as the complete and long-term crash of the New York Stock Exchange.

In the discussion of the protection of nationals abroad, it was concluded that the nonconsensual use of limited military force that is necessary and proportional to protect nationals abroad is a use of force within the meaning of Article 2(4) and that such a use of force is lawful self-defense authorized by Article 51. Given the limited scope, duration, and intensity of nonconsensual rescue operations, however, they are not an armed attack. Accordingly, it would be a lawful act of self-defense for a rescuing state to manipulate the territorial state’s computers via the Internet to electronically jam anti-aircraft fire control radars and to prevent the territorial state from detecting the rescue aircraft. It is also a lawful act of self-defense for a state to assist its nationals, who are in imminent threat of injury or harm, to escape surreptitiously from a state by manipulating that state’s database via the Internet to falsify travel documents, identity papers, passports, or other documents or databases that would facilitate their escape.
Finally, in the discussion of indirect armed force, it was concluded that those state activities in CyberSpace that either support or constitute a prohibited indirect use of force are themselves an unlawful use of force as well. For example, it would be an unlawful use of indirect force during peacetime for one state to manipulate information in another state via CyberSpace in an effort to instigate a plot to overthrow the leader of that country. It is very unlikely, however, that it would be considered an armed attack. Similarly, it would be unlawful under customary international law for a state to allow its information infrastructure to be used by another state or insurgents to engage in violent acts against a third state. It is an unlawful use of indirect force, for example, for State E to knowingly permit or acquiesce in the use of its Internet gateways by State F during peacetime to commit unlawful uses of force against State G. While mere acquiescence would not constitute an armed attack, using the information infrastructures to help arm or train insurgents in another state would constitute an armed attack.

**Conclusion**

There are no clear definitions that will define a use of force and an armed attack under all circumstances, but this chapter has provided a number of examples of state activities in CyberSpace that define the contours of what is and what is not a use of force and an armed attack within the meaning of Articles 2(4) and 51 of the Charter of the United Nations. Since these issues are very fact-dependent, the following definitions derived from this chapter’s analysis remain very general:

**Use of force.** A state activity that threatens the territorial integrity or political independence of another state constitutes an unlawful use of force within the meaning of Article 2(4) of the Charter of the United Nations.
Armed Attack. A use of force that rises to a certain scope, duration, and intensity threshold constitutes an armed attack within the meaning of Article 51 of the Charter of the United Nations that invokes a state’s inherent right of self-defense.

The best way, however, to accurately predict what may be considered a use of force and an armed attack within the meaning of Articles 2(4) and 51 is by studying state practice. In addition to traditional, universally accepted examples such as an armed cross-border invasion, an armed attack may occur when a use of force or an activity not traditionally considered an armed attack is used in such a way that it becomes tantamount in effect to an armed attack.

Figure 4 completes the development of a linear model for a heuristic use of force analysis by adding some of the examples discussed in this chapter to the spectrum of interstate relations. This figure should serve as a useful reference tool that summarizes all of the key principles discussed in Chapters 3 through 6.
Part III: State Activities in CyberSpace – Defining Use of Force and Armed Attack

Hostile

- Isolated verbal threat;
- Initial troop movements;
- Shaping of alliances;
- Initial IRBM movement.

- Massing of troops or IRBMs on border;
- Use of fire control radar;
- Interference with early warning or C² systems.

- Declared war, de facto hostilities, occupation;
- Political or economic aggression; blockade;
- Destruction of EW or C² systems;
- Use of force against territory, military forces, or citizens abroad.

Threat to the peace

Threat of force

Hostile intent

Hostile act

SPECTRUM OF INTERSTATE RELATIONS

Art. 39

Art. 2(4)

Art. 51
Chapter 6: Application of Existing Rules

121

Any measures or use of force authorized by the UNSC under Chapter VII UNSC may require states to comply with Art. 41 measures

Diplomatic measures; severance of diplomatic relations; complete or partial interruption of economic relations or interstate communications; arbitration, judicial proceedings, etc.

Art. 39

Art. 2(4)

Art. 51

Anticipatory self defense

Self defense

Jus in bello applies

Jus ad bellum applies

Peacetime regime applies
Chapter 7: Selected Issues – Computer Espionage and Computer Network Attack

Introduction

Computer espionage and computer network attack are two of the most urgent issues facing warfighters, decision-makers, and international lawyers today. While Chapter 6 examined use of force norms in CyberSpace within the legal framework of the Charter paradigm of conflict management, this chapter will in turn examine use of force norms in CyberSpace within the factual framework of these two interrelated issues.

Computer espionage

The right to conduct espionage is an essential part of a state’s inherent right of self-defense.\footnote{NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 433.} The 1907 Hague Convention IV explicitly recognizes the lawfulness of espionage during armed conflict.\footnote{See Hague Convention IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, Annex (Regulations), arts. 24, 29-31, 36 Stat. 2295, 1 Bevans 643 [hereinafter 1907 Hague Regulations], reprinted in DOCUMENTS ON THE LAWS OF WAR, supra note 2, at 48, 53-54; NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 435.} Similarly, the 1961 Vienna Convention on Diplomatic Relations explicitly recognizes the well-established right of nations to engage in espionage during peacetime, and the practice of states has specifically recognized a right to engage in such clandestine intelligence collection activities as an inherent part of foreign relations and policy.\footnote{See NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 435-36.} Espionage is, however,
unlawful under the domestic law of most states during peacetime and armed conflict.\textsuperscript{303}

What we now define as information in CyberSpace and CyberSpace infrastructures have historically been integral components of lawful espionage during peacetime and armed conflict. Customary international law, for example, has long recognized the lawfulness of the use of information in CyberSpace such as signals intelligence, communications intelligence, electronics intelligence, foreign instrumentation signals intelligence, and imagery intelligence.\textsuperscript{304} These terms are currently defined as follows:

**Signals intelligence** (SIGINT): intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.\textsuperscript{305}

**Communications intelligence** (COMINT): technical and intelligence information derived from foreign communications by other than the intended recipients.\textsuperscript{306}

**Electronics intelligence** (ELINT): technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating

\textsuperscript{303} See id. at 435.

\textsuperscript{304} See id. at 436-37.

\textsuperscript{305} Joint Pub 1-02, supra note 48, at 422.

\textsuperscript{306} Id. at 109.
from other than nuclear detonation or radioactive sources.  

**Foreign instrumentation signals intelligence** (FISINT): technical and intelligence information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems such as telemetry, beaconry, electronic interrogators, and video data links.

**Imagery intelligence** (IMINT): intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media.

Similarly, CyberSpace infrastructures such as computers, telecommunication systems, and satellites have been used for intelligence collection since their invention. The tactical and strategic use of this information in CyberSpace is embraced in the operational concept of information operations.

As a matter of domestic criminal law during peacetime, any person who is caught engaging in espionage within the criminal

---

307 *Id.* at 168.

308 *Id.* at 195.

309 *Id.* at 227.

310 *See* NATIONAL SECURITY LAW (Moore et al.), *supra* note 64, at 438-42.

311 *See* JOINT PUB 3-13, *supra* note 45, at I-9 & I-10.
jurisdiction of a state is subject to prosecution and can be exchanged for a spy of the apprehending state who has been detained by the sending state on similar charges. Should a spy have diplomatic immunity under the terms of the 1961 Vienna Convention on Diplomatic Relations, then he or she is declared *persona non grata* and sent home.

As a matter of international conflict management during peacetime, the conduct of espionage within foreign territory has caused the territorial state to use force on a number of occasions. During the period April 1950 through April 1969, for example, there were at least 22 incidents where aircraft were suspected of espionage and were attacked, mostly by the Soviet Union. During one of these incidents, a 1960 U-2 flight by the United States over Soviet territory, the Soviet government asserted that military intelligence flights by reconnaissance aircraft over Soviet territory and territorial waters are *per se* acts of aggression.

The United Nations Security Council disagreed, and concluded that the U-2 flight was a violation of Soviet airspace but not a use of force within the meaning of Article 2(4). Consistent with the Security Council’s view, one scholar has concluded that military intelligence flights may be deliberate and unlawful intrusions, but are not necessarily a use of force. Similarly,

---

312 NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 435-36.

313 Id.

314 Id. at 440-41.

315 BROWNLE, supra note 89, at 363.

316 NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 439.

317 BROWNLE, supra note 89, at 364.
another scholar has concluded that the penetration of a state’s airspace for the purposes of collection of intelligence is a violation of that state’s sovereignty but not a use of force.318 The consensus view by these and other scholars is that all nations have complete and exclusive sovereignty over their territory, however, customary international law requires a reasonable self-defense response to aircraft that violate another state’s airspace that is proportionate to the danger posed by the presence of the trespassing aircraft.319

The essence of espionage is the collection of information, and with the capabilities of today’s inter-linked computers, there is perhaps no richer source of information than what can potentially be accessed via the Internet. Some of the information is publicly available, and some must be accessed surreptitiously without the consent of the owner of the computer system. When a state accesses publicly available databases in a foreign state, no unlawful act occurs under international or domestic law. Publicly available information that has potential intelligence value is called open-source intelligence (OSINT).320

If the unlawful, physical penetration of a state’s airspace by the military aircraft of another state is not a use of force within the meaning of Article 2(4), it is certain as well that a virtual penetration of a state’s CyberSpace is not a use of force. When one state hacks into another state’s computer systems it is very likely engaging in acts that are unlawful under the domestic

318 NATIONAL SECURITY LAW (Moore et al.), supra note 64, at 439.

319 See id.; COMMANDER’S HANDBOOK, supra note 107, ¶ 4.4; BROWNLIE, supra note 89, at 363-64, 373-74. For a more detailed discussion of what force a territorial state may take in self-defense, see the previous section concerning violations of international law.

320 JOINT PUB 1-02, supra note 48, at 340.
law of the territorial state, but under international law, the hacking state may be engaging in a lawful act of espionage that may not be considered a use of force. This type of computer espionage poses a number of very serious practical problems. It may be virtually impossible, for example, for the territorial state to prosecute anyone under its domestic law for espionage since hacking can anonymously occur from almost any place in the world. A territorial state’s inability to prosecute and the almost assured anonymity of the hacking state reduces the deterrent value of domestic espionage statutes and the public embarrassment of a state getting caught spying.

Another practical problem is that once a state has penetrated another state’s information infrastructure to conduct espionage, it is only one keystroke away from the capability of engaging in hostile and potentially destructive activities that are unlawful under international law. A state’s penetration of another state’s information infrastructure may be espionage, a pre-attack exploration, or an actual attack in progress that has not yet manifested itself. Although there are some indicia of intent that can be monitored, the intentions of a state are very difficult to discern. If a trespassing state is simply looking around and copying files, for example, it may likely be engaging in nothing more than espionage. If those files, however, contained an order of battle and rules of engagement, then the trespassing state may be engaging in a pre-attack exploration of the battlefield. Similarly, if the trespassing state was planting destructive viruses and programs to facilitate future penetrations, then it may be engaged in pre-attack preparations. Finally, the planting of offensive cyber-tools may be indicative of an attack that has not yet manifested itself. Short of an actual destructive attack, however, it is very difficult for a state to be sure of the intent of a trespassing state – albeit at the minimum such a trespassing state is engaged in espionage.
The technology of computers and the Internet allows a lawful act of espionage to materialize into an unlawful use of force at the speed of light. Despite these practical problems, espionage conducted by the nonconsensual penetration of another state’s computer systems is lawful under existing international law. Regardless of whether a state committing computer espionage is about to attack immediately or if it has installed the latent hostile capability to attack with a single keystroke at some unknown point in time in the future, a legal regime that fails to recognize an ability of a state to defend itself before it has been attacked is unacceptable.

Existing law, however, does offer at least a partial solution to the threat presented by CyberSpace technology. Recall that anticipatory self-defense is permissible when “the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation.”321 There seems to be no better circumstance for anticipatory self-defense to apply than when technology allows an unlawful use of force, and potentially an armed attack, to occur literally at the speed of light. The right to respond in anticipatory self-defense does not apply to the penetration of all government computer systems during peacetime, but it should apply presumptively to those sensitive systems that are critical to a state’s vital national interests. As previously discussed, any use of force in anticipatory self-defense must be necessary and proportional under international law.

The key to this presumptive solution is a predetermination of the potential threat posed by the penetration of a specific computer system or infrastructure that is dependent upon its value to the vital national interests of a state. Remedies will, of course,

---

vary depending upon the sensitivity and importance of the penetrated computer system or infrastructure. Penetration in government computers that store personnel, logistical, or administrative data, for example, would not pose an instant and overwhelming need of anticipatory self-defense. Early detection, preventive measures, and public disclosure that results in the embarrassment of the offending state are appropriate remedies under these circumstances absent any other indications of hostile intent.

In contrast, the mere penetration by a state into sensitive computer systems such as early warning or command and control systems, missile defense computer systems, and other computers that maintain the safety and reliability of a nuclear stockpile, should by their very nature be presumed a demonstration of hostile intent. Individually, these computer systems are so important to a state’s ability to defend itself that espionage into any one of them should be presumed to demonstrate hostile intent. In these and similar cases, the necessity of self-defense may be instant, overwhelming and leaving no choice of means, and no moment for deliberation. If the identity of the intruder is known, then a victim state can evaluate the potential threat to its vital national interests and may lawfully respond in anticipatory self-defense with a necessary and proportional use of force, either in kind through CyberSpace or by more traditional uses of force. In short, all states should adopt a rule of engagement that allows them to use force in anticipatory self-defense against any identified state that demonstrates hostile intent by penetrating a computer system which is critical to their respective vital national interests. The challenge of adopting such a rule of engagement is for all states to strike the right balance between the equities of the law of conflict management and their definition of
what information infrastructures are critical to their respective vital national interests.  

The concept of vital national interests in today’s environment of information technology must include nongovernment commercial and other economic interests of a state. Almost all legal commentators would agree that a state has an unequivocal right to use force to defend the commercial infrastructure within its territory from an armed attack, and most would agree that the inherent right of self-defense includes the right of anticipatory self-defense. Computer espionage of a commercial nature by a state is an attack upon the vitality of that infrastructure and the state as a whole. Individually, these computer systems may not be so important to a state’s ability to defend itself that espionage into any one of them should be presumed to demonstrate hostile intent. A threat to these infrastructures collectively, however, is important to a state’s ability to defend itself. Accordingly, the proposed presumption should still apply to the protection of a state’s critical nongovernmental infrastructures, although the utmost care must be applied in defining when a state has the right to use force to protect them from computer espionage.

Recall from Chapter 2, for example, that the United States declared in Executive Order 13010 that eight categories of “national [commercial] infrastructures are so vital that their incapacity or destruction [by either physical or cyber attack] would have a debilitating impact on the defense or economic security of


\[323\] See id. at __.
the United States.” The key in the commercial sector is to define major portions of nongovernmental systems and infrastructures as vital national interests, not individual computers or smaller systems. Accordingly, a single bank in Kansas would not meet the definition of a vital national interest, and the United States would not have the right under international law to use force to protect that bank from a single act of espionage. If, however, there was a pattern of computer espionage that threatened the economic vitality of the national financial infrastructure of the United States, it would have the right to use necessary and proportional force in anticipatory self-defense to prevent future computer espionage.

**Computer espionage is lawful under international law and is not a use of force within the meaning of Article 2(4), however, it may demonstrate the requisite hostile intent of the intruding state necessary to invoke the victim state’s right of anticipatory self-defense.** The difficulty is to be able to determine the identity of the intruder to evaluate the seriousness of the threat presented by the penetration of these sensitive computer systems. Without the capability to identify the intruder, the legal authority to use force offers little help. Recognition by states that the penetration of some systems will be considered either an indication of hostile intent or a hostile act which authorizes a use of force in response will restore, at least in part, some deterrence. There is no better solution under the rule of law until technology can assure a rapid identification of the intruding state.

**Computer network attack**

Computer network attack (CNA) is defined as operations that “disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.”324 By definition, a computer network attack against

---

324 Joint Pub 3-13, supra note 45, at I-9.
another state will cause a destructive effect in that state. Accordingly, these operations pose a much more straightforward issue than computer espionage, and need only be addressed very briefly.

In a previous discussion, it was recognized that unarmed, non-military physical force by any agency of a state can affect another state just as severely as the use of armed military force. It was concluded in this discussion that all state activities in CyberSpace that intentionally cause any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense.

It was concluded that the scope, duration, and intensity of the force must be analyzed to determine if an armed attack has occurred and what may constitute a necessary and proportional response. Should a computer network attack cause a single train to crash, it would be an unlawful use of force but likely not an armed attack. In contrast, should a computer network attack cause dozens of such trains and aircraft to crash, it would very likely be considered an armed attack which invokes the victim state’s right to use force in self-defense. Accordingly, any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense.

Just as with computer espionage, the difficulty of responding to a computer network attack in self-defense is to be able to determine the identity of the attacking state. Without the capability of identifying the attacker, the legal authority to use force offers little help.
Conclusion

Computer espionage is lawful under international law and is not a use of force within the meaning of Article 2(4). It can, however, be an unlawful threat to use force that demonstrates the hostile intent of the intruding state and invokes the victim state's right of anticipatory self-defense. In contrast, a computer network attack that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack prompting the right of self-defense. Finally, it is important to remember that any force used in the exercise of the right of self-defense must be necessary and proportional under the circumstances.
Part IV: Conclusion

Chapter 8: Core Principles and Final Reflections

Previous chapters examined in great detail what peacetime state activities in CyberSpace constitute a threat or use of force under the Charter paradigm of conflict management, and when a use of force constitutes an armed attack within the meaning of Article 51 of the Charter. These chapters moored together a number of concepts—such as ‘threat of force,’ ‘use of force,’ ‘armed force,’ ‘armed attack,’ ‘Common Article 2 threshold,’ ‘hostile intent,’ ‘hostile act,’ ‘anticipatory self-defense,’ and ‘self-defense’—that are frequently found floating about each other, but are not conceptually linked with an internally consistent set of principles.

This final chapter will extract from these previous discussions a review of those guiding principles that form the basis for analyzing all use of force issues under international law. These guiding principles are a composite of the peacetime regime of international law, the law of conflict management, and the law of armed conflict. Application of these principles should serve as a useful starting point for an analysis of all use of force issues, to include the use of force by states in CyberSpace. Table 1 captures these principles without discussion for ease of reference.

Maintaining a credible ability to use force, in CyberSpace and elsewhere, is lawful and a fundamentally important aspect of deterrence and international peace and security. Even clearly defined norms are not adequate to control the behavior of states that continue to use aggressive force. Accordingly, peace-loving states must maintain a strong and credible ability to use force when necessary in self-defense. This ability to threaten and use force is not inherently unlawful or evil—
it is essential to the maintenance of international peace and security. Indeed, the collective use of force by the international community is the core principle upon which the Charter of the United Nations is built. International law outlaws only the aggressive use of force, and it specifically acknowledges the lawfulness of the use of force in self-defense. Maintaining the credible ability to use force is an important deterrent element that is required to ensure that the rule of law is enforced. If peace-loving states do not maintain the ability to defend themselves, individually and collectively, then international peace and security is an unachievable goal.

**International and national law governs, but does not prohibit per se, state activities that involve coercion and the use of force in CyberSpace.** At the end of every cyber-connection is a computer and a person at a particular point on earth, and that person’s behavior – whether acting individually or as a state agent – is governed by the applicable national law of where he or she resides, international law, and the national law of a foreign state where his or her behavior may have an effect. Although stirred up by CyberSpace into a complex melt of jurisdiction, conflict of law, and judgment enforcement issues, these laws are all familiar to us. They include civil law that involves tort liability and intellectual property, criminal law that proscribes trespass and theft, international law that regulates the use of force and armed conflict, and foreign domestic law that prohibits espionage or the introduction of certain political or social ideas. All state activities in CyberSpace are governed by existing international and national law.

**States have an international obligation to act in good faith in settling their disputes by peaceful means.** Any state activity in CyberSpace that
Chapter 8: Core Principles and Final Reflections

- is an act of bad faith as it pertains to that state’s dispute settlement negotiations;
- otherwise threatens a peaceful settlement of that state’s own dispute;
- interferes with a dispute of other states in such a manner that would delay or prevent their dispute settlement; or,
- creates a dispute between other states that threatens international peace and security,

violates the obligations of all Member States under Article 2(3) of the Charter of the United Nations to “settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.”

Articles 2(4), 39, and 51 of the Charter of the United Nations now redefine and codify the contemporary *jus ad bellum* in its entirety. For four millennia, war has been accepted as a legitimate form of violence. Not until the establishment of the Charter of the United Nations was the aggressive use of force outlawed and punishable as a crime against peace.

If a state activity is a use of force within the meaning of Article 2(4), it is unlawful unless it is an exercise of that state’s inherent right of self-defense or unless it is authorized by the Security Council under its coercive Chapter VII authority. While the aggressive use of force was specifically outlawed, states reserved their inherent right to use force in individual and collective self-defense. The international community has conferred upon the Security Council the primary responsibility for the maintenance of international peace, and the power to authorize the use of military force to eliminate breaches of the peace, acts of aggression, and threats to international peace and security.

What constitutes a prohibited ‘threat or use of force,’ in CyberSpace and elsewhere, is a question of fact that must be
subjectively analyzed in each and every case in the context of all relevant law and circumstances. The terms ‘use of force,’ ‘armed attack,’ and ‘self-defense’ will never be clearly defined by objective rules of law. The international community has struggled for decades to define these terms, but there are simply too many factual variables involved to capture them in a few simple rules. Almost all attempts by statesmen and scholars to craft generally accepted, objective definitions, and certainly all of those in the mainstream of international legal thought, are qualified by exceptions consistent with the principles discussed in this book and summarized in this chapter.

The best way to accurately predict what may be considered an armed attack within the meaning of Article 51 is by studying state practice. In addition to traditional, universally accepted examples such as an armed cross-border invasion, an armed attack may occur when a use of force or an activity not traditionally considered an armed attack is used in such a way that it becomes tantamount in effect to an armed attack. There is no clear definition of armed attack, but Chapter 6 provided a number of examples of state activities in CyberSpace that define what is and what is not an armed attack within the meaning of Article 51 of the Charter.

An international armed conflict exists upon the declaration of war, the occurrence of de facto hostilities between two or more contracting parties even if the state of war is not recognized by one of them, and in all cases of partial or total occupation even if met with no armed resistance. This restatement of the Common Article 2 threshold is universally accepted as the test for when an international armed conflict exists.

De facto hostilities exist between two states when the scope, duration, and intensity of force between them reaches the level of an armed attack within the meaning of Article 51 of
the Charter. What constitutes a use of force of a scope, duration, and intensity that constitutes an armed attack and triggers the *jus in bello* is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances.

A use of force within the meaning of Article 2(4) may not always rise to the scope, duration, and intensity threshold of an armed attack that invokes a *de facto* international armed conflict and the *jus in bello*. This is based upon the universally accepted view that the thresholds of Articles 2(4) and 51 are different in scope, *i.e.*, the Article 2(4) concept of a threat or use of force is much broader than the more restrictive Article 51 threshold of armed attack.

A state never loses its right to use force in self-defense in response to a use of force within the meaning of Article 2(4), however, the right of self-defense under customary international law may not always justify an armed response. There are no circumstances under which a state does not have the right to self-defense when provoked by a use of force within the meaning of Article 2(4). The right of self-defense, however, is not unlimited. A claim to self-defense must be reasonable under the circumstances, but what constitutes a threat or use of force that invokes the right of self-defense must be evaluated from the subjective perspective of the state claiming self-defense. All lawful uses of force must be necessary and proportional to the threat, which may mean that an armed response is not appropriate under the customary international law of self-defense. Until such time that the Security Council is able to take effective measures to remove the threat, all states retain the right to use all necessary force in individual and collective self-defense.

State activities in CyberSpace that constitute a use of force within the meaning of Article 2(4) may be conducted by
any state agent – not just the military. Unarmed, non-military physical force can affect another state just as severely as the use of armed military force. State activities must be analyzed in light of their effect on another state, and not what agency of the state is responsible for the state activity.

Computer espionage is lawful under international law and is not a use of force within the meaning of Article 2(4); however, it may demonstrate the requisite hostile intent of the intruding state necessary to invoke the victim state’s right of anticipatory self-defense. The difficulty is to be able to determine the identity of the intruder to evaluate the seriousness of the threat presented by the penetration of sensitive computer systems. Without the capability of identifying the intruder, the legal authority to use force offers little help.

Any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense. This is a relatively straightforward analysis for determining when a computer network attack constitutes an unlawful use of force. Just as with computer espionage, the difficulty of responding to a computer network attack in self-defense is to be able to determine the identity of the attacking state.

All planned state activities in CyberSpace should be reviewed by assigned government counsel. The complexity of the application of international, U.S. domestic, and foreign law during the conduct of state activities in CyberSpace requires prudent decision-makers to have their attorneys present whenever possible in all phases of planning and operations. In the military, a legal review of all information operations is required. An
instruction from the Chairman of the Joint Chiefs of Staff provides that information operations

conducted throughout the range of military operations may involve complex legal issues. The complexities introduced by domestic, foreign, and international law make it critical that at the appropriate level of command legal counsel is involved in policy development as well as the development and employment of various techniques and capabilities. Military technologies, tactics, techniques, and procedures for conducting IO must undergo a legal review in accordance with reference e to ensure that they are consistent with the domestic and international legal obligations of the United States.325

This complexity permits legal advisers to support the proposed activities of their clients with many meritorious arguments of lawfulness. They must also, however, advise their clients of potential allegations of unlawfulness to prevent adverse consequences that may undermine their client’s positions and national goals. Finally, legal advisers must fully understand the science and technology that is behind the military applications of CyberSpace – simply knowing the law is not enough.

Technology and the practice of states will shape the evolution of law that governs information operations. The international community must be guided by principles that evolve with technology and state practice. If good faith is exercised in applying the existing principles of the law of conflict management to the use of force in CyberSpace, then a reasonable regime will emerge out of state practice.

Although there is a considerable body of international law that governs the use of force in CyberSpace, technology does not allow a state to completely prevent computer espionage or computer network attack, nor does it assure that a state can reliably determine the identity of an intruder or attacker in any timely manner. This shortcoming in technology limits a state’s ability to use force in self-defense. The real exigency facing warfighters and decision-makers is whether timely intelligence and technology will allow a state to respond by identifying an intruding or attacking state, not whether international law will permit a use of force in self-defense.
### USE OF FORCE PRINCIPLES

**Table 1**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintaining a credible ability to use force in CyberSpace is lawful and a</td>
<td>International and national law governs, but does not prohibit per se, state activities that involve coercion and the use of force in CyberSpace.</td>
</tr>
<tr>
<td>fundamentally important aspect of deterrence and international peace and</td>
<td>States have an international obligation to act in good faith in settling their disputes by peaceful means.</td>
</tr>
<tr>
<td>security.</td>
<td>Articles 2(4), 39, and 51 of the Charter of the United Nations now redefine and codify the contemporary <em>jus ad bellum</em> in its entirety.</td>
</tr>
<tr>
<td>If a state activity is a use of force within the meaning of Article 2(4),</td>
<td>What constitutes a prohibited ‘threat or use of force’ in CyberSpace is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances.</td>
</tr>
<tr>
<td>it is unlawful unless it is an exercise of that state’s inherent right of</td>
<td>The best way to accurately predict what may be considered an armed attack within the meaning of Article 51 is by studying state practice.</td>
</tr>
<tr>
<td>self-defense or unless it is authorized by the Security Council under its</td>
<td>An international armed conflict exists upon the declaration of war, the occurrence of <em>de facto</em> hostilities between two or more contracting parties even if the state of war is not recognized by one of them, and in all cases of partial or total occupation even if met with no armed resistance.</td>
</tr>
<tr>
<td>coercive Chapter VII authority.</td>
<td><em>De facto</em> hostilities exist between two states when the scope, duration, and intensity of force between them reaches the level of an armed attack within the meaning of Article 51 of the Charter.</td>
</tr>
<tr>
<td>A use of force within the meaning of Article 2(4) may not always rise to</td>
<td>A state never loses its right to use force in self-defense in response to a use of force within the meaning of Article 2(4), however, the right of self-defense under customary international law may not always justify an armed response.</td>
</tr>
<tr>
<td>the scope, duration, and intensity threshold of an armed attack that invokes</td>
<td>State activities in CyberSpace that constitute a use of force within the meaning of Article 2(4) may be conducted by any state agent – not just the military.</td>
</tr>
<tr>
<td>a <em>de facto</em> international armed conflict and the <em>jus in bello</em>.</td>
<td>Computer espionage is lawful under international law and is not a use of force within the meaning of Article 2(4); however, it may demonstrate the requisite hostile intent of the intruding state necessary to invoke the victim state’s right of anticipatory self-defense.</td>
</tr>
<tr>
<td>Any CNA that intentionally causes any destructive effect within the</td>
<td>All planned state activities in CyberSpace should be reviewed by assigned government counsel.</td>
</tr>
<tr>
<td>sovereign territory of another state is an unlawful use of force within</td>
<td>Technology and the practice of states will shape the evolution of law that governs IO.</td>
</tr>
</tbody>
</table>
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Civil affairs</td>
</tr>
<tr>
<td>COMINT</td>
<td>Communications intelligence</td>
</tr>
<tr>
<td>CNA</td>
<td>Computer network attack</td>
</tr>
<tr>
<td>ELINT</td>
<td>Electronics intelligence</td>
</tr>
<tr>
<td>EA</td>
<td>Electronic attack</td>
</tr>
<tr>
<td>EW</td>
<td>Electronic warfare</td>
</tr>
<tr>
<td>EP</td>
<td>Electronic protection</td>
</tr>
<tr>
<td>ES</td>
<td>Electronic warfare support</td>
</tr>
<tr>
<td>FISINT</td>
<td>Foreign instrumentation signals intelligence</td>
</tr>
<tr>
<td>ICJ</td>
<td>International Court of Justice</td>
</tr>
<tr>
<td>ICRC</td>
<td>International Committee of the Red Cross</td>
</tr>
<tr>
<td>IMINT</td>
<td>Imagery intelligence</td>
</tr>
<tr>
<td>IO</td>
<td>Information operations</td>
</tr>
<tr>
<td>IW</td>
<td>Information warfare</td>
</tr>
<tr>
<td>LOAC</td>
<td>Law of armed conflict</td>
</tr>
<tr>
<td>LOCM</td>
<td>Law of conflict management</td>
</tr>
<tr>
<td>LOIC</td>
<td>Law of information conflict</td>
</tr>
<tr>
<td>OPSEC</td>
<td>Operations security</td>
</tr>
<tr>
<td>OSINT</td>
<td>Open-source intelligence</td>
</tr>
<tr>
<td>PA</td>
<td>Public affairs</td>
</tr>
<tr>
<td>PSYOP</td>
<td>Psychological operation</td>
</tr>
<tr>
<td>ROE</td>
<td>Rules of engagement</td>
</tr>
<tr>
<td>SIGINT</td>
<td>Signals intelligence</td>
</tr>
<tr>
<td>SROE</td>
<td>Standing Rules of Engagement</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
</tbody>
</table>
GLOSSARY

**Aggressive use of force.** Generally, the word aggressive refers to beginning a dispute by being the first to either threaten or use force. See BLACK’S LAW DICTIONARY, supra note 15, at 60. For the purposes of this book, an ‘aggressive use of force’ is a shorthand term used to refer to any use of force within the meaning of Article 2(4) that is not justified by a state’s right of self-defense or authorized by the Security Council under its coercive Chapter VII powers.

**Anticipatory self-defense.** Authorizes the use of force in self-defense at that point in time before an attack occurs when “the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation.” See THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 675. See “hostile intent,” this glossary.

**Armed attack.** A use of force that rises to a certain scope, duration, and intensity threshold within the meaning of Article 51 of the Charter of the United Nations that invokes a state’s inherent right of self-defense.

**Armed conflict.** A state of de facto hostilities invoked by the use of force by one party without any formal declaration of war. DOCUMENTS ON THE LAWS OF WAR, supra note 2, at 1-2. See “war,” this glossary.

**Armed force.** Generally used to refer to military force involving the use of weapons, but is interpreted very broadly under international law to include non-military physical force, indirect force, and other forms of coercion that are tantamount in effect to an armed attack.
Civil affairs (CA). The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. JOINT PUB 1-02, supra note 48, at 91.

Common Article 2. An article common to the four Geneva Conventions of 1949 that is widely accepted as the threshold test for when an international armed conflict exists, and consequently, when the law of armed conflict applies. The Common Article 2 threshold thus determines the transition point between peace and armed conflict.

Communications intelligence (COMINT). Technical and intelligence information derived from foreign communications by other than the intended recipients. JOINT PUB 1-02, supra note 48, at 109.

Computer espionage. The act through the medium of CyberSpace of obtaining, delivering, transmitting, communicating, or receiving information about the national defense of a state with an intent, or reason to believe, that the information may be used to the injury of that state or to the advantage of any foreign nation.

Computer network attack (CNA). Operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. JOINT PUB 3-13, supra note 45, at I-9. See also JOINT PUB 1-02, supra note 48, at 112.
**Covert operation.** An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. A covert operation differs from a clandestine operation in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation. **Joint Pub 1-02, supra** note 48, at 129.

**CyberSpace.** The environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web.

**Dicta.** Opinions of a judge which do not embody the resolution or determination of the court. Expressions in court’s opinion which go beyond the facts before court and therefore are individual views of author of opinion and not binding in subsequent cases. **Black’s Law Dictionary, supra** note 15, at 408.

**Electronics intelligence (ELINT).** Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonation or radioactive sources. **Joint Pub 1-02, supra** note 48, at 168.

**Electronic warfare (EW).** Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

  a. **Electronic attack (EA).** That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes:
1) actions taken to prevent or reduce an enemy’s effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and
2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

b. Electronic protection (EP). That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

c. Electronic warfare support (ES). That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronics intelligence.

JOINT PUB 1-02, supra note 48, at 168.

Espionage. The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense of a state with an intent, or reason to believe, that the information may be used to the injury of that state or to the advantage of any foreign nation. See JOINT PUB 1-02, supra note 48, at 174.

Foreign instrumentation signals intelligence (FISINT). Technical and intelligence information derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and
subsurface systems such as telemetry, beaconry, electronic interrogators, and video data links. JOINT PUB 1-02, supra note 48, at 195.

**Hostile act.** An attack or other use of force by a foreign force or terrorist unit (organization or individual) against the United States, U.S. forces, and in certain circumstances, U.S. citizens, their property, U.S. commercial assets, and other designated non-U.S. forces, foreign nationals and their property. It is also force used directly to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel and vital U.S. Government property. When a hostile act is in progress, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. CJCSI 3121.01, supra note 237, Encl. A, para. 5e.

**Hostile intent.** The threat of imminent use of force by a foreign force or terrorist unit (organization or individual) against the United States, U.S. forces, and in certain circumstances, U.S. citizens, their property, U.S. commercial assets, or other designated non-U.S. forces, foreign nationals and their property. When hostile intent is present, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. CJCSI 3121.01, supra note 237, Encl. A, para. 5f.

**Imagery intelligence (IMINT).** Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. JOINT PUB 1-02, supra note 48, at 227.
Information operations (IO). Actions taken to affect adversary information and information systems while defending one’s own information and information systems. JOINT PUB 1-02, supra note 48, at 234.

Information warfare (IW). Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. JOINT PUB 1-02, supra note 48, at 234.

Infra. Below, under, beneath, underneath. This word occurring by itself in a book refers the reader to a later part of the book. BLACK’S LAW DICTIONARY, supra note 15, at 701.

International armed conflict. An armed conflict between two or more sovereign states.

International Court of Justice (ICJ). The judicial arm of the United Nations. It has the jurisdiction to give advisory opinions on matters of law and treaty construction when requested by the General Assembly, Security Council or any other international agency so authorized by the General Assembly. It has jurisdiction, also, to settle legal disputes between nations when voluntarily submitted to it. Its judgments may be enforced by the Security Council. BLACK’S LAW DICTIONARY, supra note 15, at 732.

International law. The law which regulates the intercourse of nations; the law of nations. The customary law which determines the rights and regulates the intercourse of independent nations in peace and war. BLACK’S LAW DICTIONARY, supra note 15, at 733.

Internet. A cooperatively-run global network of computers with a common addressing scheme linked by telecommunication infrastructures.
**Ipso facto.** (Latin) By the fact itself; by the mere fact. By the mere effect of an act or a fact. BLACK’S LAW DICTIONARY, *supra* note 15, at 743.


**Jus ad bellum.** (Latin) The law of conflict management.

**Jus in bello.** (Latin) The law of armed conflict.

**Law of armed conflict (LOAC).** A set of rules under international law that govern the actual conduct of hostilities. Also generally referred to as the law of war. See “law of war,” this glossary.

**Law of conflict management (LOCM).** A set of rules under international law that govern the use of force between states and determine whether a conflict is lawful or unlawful in its inception.

**Law of information conflict (LOIC).** The composite of the peacetime regime of international law, the law of conflict management, and the law of armed conflict that regulates the conduct of all state activities in CyberSpace.

**Law of war.** This term comprises the body of rules and principles observed by civilized nations for the regulation of matters inherent in, or incidental to, the conduct of a public war; such, for example, as the relations of neutrals and belligerents, blockades, captures, prizes, truces and armistices, capitulations, prisoners, and declarations of war and peace. BLACK’S LAW DICTIONARY, *supra* note 15, at 1419-20. Also generally referred to as the law of armed conflict.
**Line of belligerency.** The point on the use of force spectrum at which international armed conflicts begin and the law of armed conflict applies. This point is triggered by the declaration of war, the occurrence of *de facto* hostilities, and all cases of partial or total occupation.

**Military deception.** Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are strategic military deception, operational military deception, tactical military deception, Service military deception, and military deception in support of operations security. JOINT PUB 1-02, *supra* note 48, at 298.

**Open-source intelligence (OSINT).** Information of potential intelligence value that is available to the general public. JOINT PUB 1-02, *supra* note 48, at 340.

**Operations security (OPSEC).** A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.
b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

JOINT PUB 1-02, *supra* note 48, at 343.
Prima facie. (Latin) At first sight; on the face of it; a fact presumed to be true unless disproved by some evidence to the contrary. BLACK’S LAW DICTIONARY, supra note 15, at 1071.

Psychological operation (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives. JOINT PUB 1-02, supra note 48, at 375.

Public affairs (PA). Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. JOINT PUB 1-02, supra note 48, at 375.

Reprisal. An act which is unlawful per se, unless it can be justified as a counter-measure triggered by an unlawful act and is designed to induce the offending state to return to full compliance with the law. The right of reprisal does not include the right to unlawfully use force contrary to Article 2(4) of the Charter. THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, supra note 68, at 105.

Retortion. Generally, when a state unlawfully subjects citizens of another state to severe and stringent regulations or harsh treatment in response to similar unlawful mistreatment of its own citizens. See BLACK’S LAW DICTIONARY, supra note 15, at 1183.

Rules of engagement (ROE). Directives issued by competent military authority which delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. JOINT PUB 1-02, supra note 48, at 403.
Self-defense. The protection of person or property against some injury attempted by another. [Generally, under U.S. domestic law,] the law of “self-defense” justifies an act done in the reasonable belief of immediate danger, and, if an injury was done by defendant in justifiable self-defense, he can never be punished criminally nor held responsible for damages in a civil action. BLACK’S LAW DICTIONARY, supra note 15, at 1219-20.

Signals intelligence (SIGINT). Intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. joint pub 1-02, supra note 48, at 422.

Standing Rules of Engagement for US Forces (SROE). The document approved by the U.S. Secretary of Defense which provides implementation guidance on the inherent right and obligation of self-defense and the application of force for mission accomplishment. The SROE establish fundamental policies and procedures governing the actions to be taken by U.S. force commanders during all military operations, contingencies, or prolonged conflicts. CJCSI 3121.01, supra note 237, Encl. A, para. 1a.

Stare decisis. (Latin) To abide by, or adhere to, decided cases. Policy of courts to stand by precedent and not to disturb a settled point of law. BLACK’S LAW DICTIONARY, supra note 15, at 1261.

Supra. (Latin) Above; upon. This word occurring by itself in a book refers the reader to a previous part of the book. BLACK’S LAW DICTIONARY, supra note 15, at 1291.
**Threat of force.** An express or implied promise by a government of a resort to force conditional on non-acceptance of certain demands of that government. BROWNLIE, supra note 89, at 364.

**Use of force.** A state activity that threatens the territorial integrity or political independence of another state within the meaning of Article 2(4) of the Charter of the United Nations.

**War.** A state of *de jure* hostilities invoked by a formal declaration of one party (DOCUMENTS ON THE LAWS OF WAR, supra note 2, at 1-2) that creates an international armed conflict as a matter of law (FM 27-10, supra note 152, ¶ 8). A contest by force between two or more nations, carried on for any purpose, or armed conflict of sovereign powers or declared and open hostilities, or the state of nations among whom there is an interruption of pacific relations, and a general contention by force, authorized by the sovereign. BLACK’S LAW DICTIONARY, supra note 15, at 1419. See “armed conflict,” this glossary.

**World Wide Web (WWW).** A collection of files and databases linked by hypertext that was created in 1989 as the primary platform of the Internet that translates diverse computer protocols into standard format.
DOCUMENT ANNEX
DOCUMENT A

THE CHARTER OF THE UNITED NATIONS


Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Articles</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Purposes and Principles</td>
<td>1-2</td>
</tr>
<tr>
<td>II. Membership</td>
<td>3-6</td>
</tr>
<tr>
<td>III. Organs</td>
<td>7-8</td>
</tr>
<tr>
<td>IV. The General Assembly</td>
<td>9-22</td>
</tr>
<tr>
<td>V. The Security Council</td>
<td>23-32</td>
</tr>
<tr>
<td>VI. Pacific Settlement of Disputes</td>
<td>33-38</td>
</tr>
<tr>
<td>VII. Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression</td>
<td>39-51</td>
</tr>
<tr>
<td>VIII. Regional Arrangements</td>
<td>52-54</td>
</tr>
<tr>
<td>IX. International Economic and Social Co-Operation</td>
<td>55-60</td>
</tr>
<tr>
<td>X. The Economic and Social Council</td>
<td>61-72</td>
</tr>
<tr>
<td>XI. Declaration Regarding Non-Self-Governing Territories</td>
<td>73-74</td>
</tr>
<tr>
<td>XII. International Trusteeship System</td>
<td>75-85</td>
</tr>
<tr>
<td>XIII. The Trusteeship Council</td>
<td>86-91</td>
</tr>
<tr>
<td>XIV. The International Court of Justice</td>
<td>92-96</td>
</tr>
<tr>
<td>XV. The Secretariat</td>
<td>97-101</td>
</tr>
<tr>
<td>XVI. Miscellaneous Provisions</td>
<td>102-105</td>
</tr>
<tr>
<td>XVII. Transitional Security Arrangements</td>
<td>106-107</td>
</tr>
<tr>
<td>XVIII. Amendments</td>
<td>108-109</td>
</tr>
<tr>
<td>XIX. Ratification and Signature</td>
<td>110-111</td>
</tr>
</tbody>
</table>
PREAMBLE

WE THE PEOPLES
OF THE UNITED NATIONS
DETERMINED

to save succeeding generations from the scourge of war, which
twice in our lifetime has brought untold sorrow to mankind, and

to reaffirm faith in fundamental human rights, in the dignity and
worth of the human person, in the equal rights of men and women
and of nations large and small, and

to establish conditions under which justice and respect for the
obligations arising from treaties and other sources of international
law can be maintained, and

to promote social progress and better standards of life in larger
freedom,

AND FOR THESE ENDS

to practice tolerance and live together in peace with one another as
good neighbours, and

to unite our strength to maintain international peace and security,
and

to ensure, by the acceptance of principles and the institution of
methods, that armed force shall not be used, save in the common
interest, and

to employ international machinery for the promotion of the
economic and social advancement of all peoples,
HAVE RESOLVED TO COMBINE OUR EFFORTS TO
ACCOMPLISH THESE AIMS

Accordingly, our respective Governments, through representatives
assembled in the city of San Francisco, who have exhibited their
full powers found to be in good and due form, have agreed to the
present Charter of the United Nations and do hereby establish an
international organization to be known as the United Nations.

CHAPTER I

PURPOSES AND PRINCIPLES

Article 1

The Purposes of the United Nations are:

1. To maintain international peace and security, and to that end: to
take effective collective measures for the prevention and removal
of threats to the peace, and for the suppression of acts of
aggression or other breaches of the peace, and to bring about by
peaceful means, and in conformity with the principles of justice
and international law, adjustment or settlement of international
disputes or situations which might lead to a breach of the peace;

2. To develop friendly relations among nations based on respect
for the principle of equal rights and self-determination of peoples,
and to take other appropriate measures to strengthen universal
peace;

3. To achieve international co-operation in solving international
problems of an economic, social, cultural, or humanitarian
character, and in promoting and encouraging respect for human
rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.

**Article 2**

The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles:

1. The Organization is based on the principle of the sovereign equality of all its Members.

2. All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfil in good faith the obligations assumed by them in accordance with the present Charter.

3. All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.

4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

5. All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action.
6. The Organization shall ensure that states which are not Members of the United Nations act in accordance with these Principles so far as may be necessary for the maintenance of international peace and security.

7. Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.

CHAPTER II

MEMBERSHIP

Article 3

The original Members of the United Nations shall be the states which, having participated in the United Nations Conference on International Organization at San Francisco, or having previously signed the Declaration by United Nations of 1 January 1942, sign the present Charter and ratify it in accordance with Article 110.

Article 4

1. Membership in the United Nations is open to all other peace-loving states which accept the obligations contained in the present Charter and, in the judgment of the Organization, are able and willing to carry out these obligations.

2. The admission of any such state to membership in the United Nations will be effected by a decision of the General Assembly upon the recommendation of the Security Council.
Article 5

A Member of the United Nations against which preventive or enforcement action has been taken by the Security Council may be suspended from the exercise of the rights and privileges of membership by the General Assembly upon the recommendation of the Security Council. The exercise of these rights and privileges may be restored by the Security Council.

Article 6

A Member of the United Nations which has persistently violated the Principles contained in the present Charter may be expelled from the Organization by the General Assembly upon the recommendation of the Security Council.

CHAPTER III

ORGANS

Article 7

1. There are established as the principal organs of the United Nations: a General Assembly, a Security Council, an Economic and Social Council, a Trusteeship Council, an International Court of Justice, and a Secretariat.

2. Such subsidiary organs as may be found necessary may be established in accordance with the present Charter.
Article 8

The United Nations shall place no restrictions on the eligibility of men and women to participate in any capacity and under conditions of equality in its principal and subsidiary organs.

CHAPTER IV

THE GENERAL ASSEMBLY

COMPOSITION

Article 9

1. The General Assembly shall consist of all the Members of the United Nations.

2. Each Member shall have not more than five representatives in the General Assembly.

FUNCTIONS AND POWERS

Article 10

The General Assembly may discuss any questions or any matters within the scope of the present Charter or relating to the powers and functions of any organs provided for in the present Charter, and, except as provided in Article 12, may make recommendations to the Members of the United Nations or to the Security Council or to both on any such questions or matters.
Article 11

1. The General Assembly may consider the general principles of co-operation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments, and may make recommendations with regard to such principles to the Members or to the Security Council or to both.

2. The General Assembly may discuss any questions relating to the maintenance of international peace and security brought before it by any Member of the United Nations, or by the Security Council, or by a state which is not a Member of the United Nations in accordance with Article 35, paragraph 2, and, except as provided in Article 12, may make recommendations with regard to any such questions to the state or states concerned or to the Security Council or to both. Any such question on which action is necessary shall be referred to the Security Council by the General Assembly either before or after discussion.

3. The General Assembly may call the attention of the Security Council to situations which are likely to endanger international peace and security.

4. The powers of the General Assembly set forth in this Article shall not limit the general scope of Article 10.

Article 12

1. While the Security Council is exercising in respect of any dispute or situation the functions assigned to it in the present Charter, the General Assembly shall not make any recommendation with regard to that dispute or situation unless the Security Council so requests.
2. The Secretary-General, with the consent of the Security Council, shall notify the General Assembly at each session of any matters relative to the maintenance of international peace and security which are being dealt with by the Security Council and shall similarly notify the General Assembly, or the Members of the United Nations if the General Assembly is not in session, immediately the Security Council ceases to deal with such matters.

Article 13

1. The General Assembly shall initiate studies and make recommendations for the purpose of:

a. promoting international co-operation in the political field and encouraging the progressive development of international law and its codification;

b. promoting international co-operation in the economic, social, cultural, educational, and health fields, and assisting in the realization of human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion.

2. The further responsibilities, functions and powers of the General Assembly with respect to matters mentioned in paragraph 1 (b) above are set forth in Chapters IX and X.

Article 14

Subject to the provisions of Article 12, the General Assembly may recommend measures for the peaceful adjustment of any situation, regardless of origin, which it deems likely to impair the general welfare or friendly relations among nations, including situations resulting from a violation of the provisions of the present Charter setting forth the Purposes and Principles of the United Nations.
**Article 15**

1. The General Assembly shall receive and consider annual and special reports from the Security Council; these reports shall include an account of the measures that the Security Council has decided upon or taken to maintain international peace and security.

2. The General Assembly shall receive and consider reports from the other organs of the United Nations.

**Article 16**

The General Assembly shall perform such functions with respect to the international trusteeship system as are assigned to it under Chapters XII and XIII, including the approval of the trusteeship agreements for areas not designated as strategic.

**Article 17**

1. The General Assembly shall consider and approve the budget of the Organization.

2. The expenses of the Organization shall be borne by the Members as apportioned by the General Assembly.

3. The General Assembly shall consider and approve any financial and budgetary arrangements with specialized agencies referred to in Article 57 and shall examine the administrative budgets of such specialized agencies with a view to making recommendations to the agencies concerned.
VOTING

Article 18

1. Each member of the General Assembly shall have one vote.

2. Decisions of the General Assembly on important questions shall be made by a two-thirds majority of the members present and voting. These questions shall include: recommendations with respect to the maintenance of international peace and security, the election of the non-permanent members of the Security Council, the election of the members of the Economic and Social Council, the election of members of the Trusteeship Council in accordance with paragraph 1 (c) of Article 86, the admission of new Members to the United Nations, the suspension of the rights and privileges of membership, the expulsion of Members, questions relating to the operation of the trusteeship system, and budgetary questions.

3. Decisions on other questions, including the determination of additional categories of questions to be decided by a two-thirds majority, shall be made by a majority of the members present and voting.

Article 19

A Member of the United Nations which is in arrears in the payment of its financial contributions to the Organization shall have no vote in the General Assembly if the amount of its arrears equals or exceeds the amount of the contributions due from it for the preceding two full years. The General Assembly may, nevertheless, permit such a Member to vote if it is satisfied that the failure to pay is due to conditions beyond the control of the Member.
PROCEDURE

Article 20

The General Assembly shall meet in regular annual sessions and in such special sessions as occasion may require. Special sessions shall be convoked by the Secretary-General at the request of the Security Council or of a majority of the Members of the United Nations.

Article 21

The General Assembly shall adopt its own rules of procedure. It shall elect its President for each session.

Article 22

The General Assembly may establish such subsidiary organs as it deems necessary for the performance of its functions.

CHAPTER V

THE SECURITY COUNCIL

COMPOSITION

Article 23

Assembly shall elect ten other Members of the United Nations to be non-permanent members of the Security Council, due regard being specially paid, in the first instance to the contribution of Members of the United Nations to the maintenance of international peace and security and to the other purposes of the Organization, and also to equitable geographical distribution.

2. The non-permanent members of the Security Council shall be elected for a term of two years. In the first election of the non-permanent members after the increase of the membership of the Security Council from eleven to fifteen, two of the four additional members shall be chosen for a term of one year. A retiring member shall not be eligible for immediate re-election.

3. Each member of the Security Council shall have one representative.

FUNCTIONS AND POWERS

Article 24

1. In order to ensure prompt and effective action by the United Nations, its Members confer on the Security Council primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf.

2. In discharging these duties the Security Council shall act in accordance with the Purposes and Principles of the United Nations. The specific powers granted to the Security Council for the discharge of these duties are laid down in Chapters VI, VII, VIII, and XII.

3. The Security Council shall submit annual and, when necessary, special reports to the General Assembly for its consideration.
Article 25

The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.

Article 26

In order to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources, the Security Council shall be responsible for formulating, with the assistance of the Military Staff Committee referred to in Article 47, plans to be submitted to the Members of the United Nations for the establishment of a system for the regulation of armaments.

VOTING

Article 27

1. Each member of the Security Council shall have one vote.

2. Decisions of the Security Council on procedural matters shall be made by an affirmative vote of nine members.

3. Decisions of the Security Council on all other matters shall be made by an affirmative vote of nine members including the concurring votes of the permanent members; provided that, in decisions under Chapter VI, and under paragraph 3 of Article 52, a party to a dispute shall abstain from voting.
PROCEDURE

Article 28

1. The Security Council shall be so organized as to be able to function continuously. Each member of the Security Council shall for this purpose be represented at all times at the seat of the Organization.

2. The Security Council shall hold periodic meetings at which each of its members may, if it so desires, be represented by a member of the government or by some other specially designated representative.

3. The Security Council may hold meetings at such places other than the seat of the Organization as in its judgment will best facilitate its work.

Article 29

The Security Council may establish such subsidiary organs as it deems necessary for the performance of its functions.

Article 30

The Security Council shall adopt its own rules of procedure, including the method of selecting its President.

Article 31

Any Member of the United Nations which is not a member of the Security Council may participate, without vote, in the discussion of any question brought before the Security Council whenever the
latter considers that the interests of that Member are specially affected.

**Article 32**

Any Member of the United Nations which is not a member of the Security Council or any state which is not a Member of the United Nations, if it is a party to a dispute under consideration by the Security Council, shall be invited to participate, without vote, in the discussion relating to the dispute. The Security Council shall lay down such conditions as it deems just for the participation of a state which is not a Member of the United Nations.

**CHAPTER VI**

**PACIFIC SETTLEMENT OF DISPUTES**

**Article 33**

1. The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.

2. The Security Council shall, when it deems necessary, call upon the parties to settle their dispute by such means.

**Article 34**

The Security Council may investigate any dispute, or any situation which might lead to international friction or give rise to a dispute, in order to determine whether the continuance of the dispute or
situation is likely to endanger the maintenance of international peace and security.

**Article 35**

1. Any Member of the United Nations may bring any dispute, or any situation of the nature referred to in Article 34, to the attention of the Security Council or of the General Assembly.

2. A state which is not a Member of the United Nations may bring to the attention of the Security Council or of the General Assembly any dispute to which it is a party if it accepts in advance, for the purposes of the dispute, the obligations of pacific settlement provided in the present Charter.

3. The proceedings of the General Assembly in respect of matters brought to its attention under this Article will be subject to the provisions of Articles 11 and 12.

**Article 36**

1. The Security Council may, at any stage of a dispute of the nature referred to in Article 33 or of a situation of like nature, recommend appropriate procedures or methods of adjustment.

2. The Security Council should take into consideration any procedures for the settlement of the dispute which have already been adopted by the parties.

3. In making recommendations under this Article the Security Council should also take into consideration that legal disputes should as a general rule be referred by the parties to the International Court of Justice in accordance with the provisions of the Statute of the Court.
Article 37

1. Should the parties to a dispute of the nature referred to in Article 33 fail to settle it by the means indicated in that Article, they shall refer it to the Security Council.

2. If the Security Council deems that the continuance of the dispute is in fact likely to endanger the maintenance of international peace and security, it shall decide whether to take action under Article 36 or to recommend such terms of settlement as it may consider appropriate.

Article 38

Without prejudice to the provisions of Articles 33 to 37, the Security Council may, if all the parties to any dispute so request, make recommendations to the parties with a view to a pacific settlement of the dispute.

CHAPTER VII

ACTION WITH RESPECT TO THREATS TO THE PEACE, BREACHES OF THE PEACE, AND ACTS OF AGGRESSION

Article 39

The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.
Article 40

In order to prevent an aggravation of the situation, the Security Council may, before making the recommendations or deciding upon the measures provided for in Article 39, call upon the parties concerned to comply with such provisional measures as it deems necessary or desirable. Such provisional measures shall be without prejudice to the rights, claims, or position of the parties concerned. The Security Council shall duly take account of failure to comply with such provisional measures.

Article 41

The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

Article 42

Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.
Article 43

1. All Members of the United Nations, in order to contribute to the maintenance of international peace and security, undertake to make available to the Security Council, on its call and in accordance with a special agreement or agreements, armed forces, assistance, and facilities, including rights of passage, necessary for the purpose of maintaining international peace and security.

2. Such agreement or agreements shall govern the numbers and types of forces, their degree of readiness and general location, and the nature of the facilities and assistance to be provided.

3. The agreement or agreements shall be negotiated as soon as possible on the initiative of the Security Council. They shall be concluded between the Security Council and Members or between the Security Council and groups of Members and shall be subject to ratification by the signatory states in accordance with their respective constitutional processes.

Article 44

When the Security Council has decided to use force it shall, before calling upon a Member not represented on it to provide armed forces in fulfilment of the obligations assumed under Article 43, invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces.

Article 45

In order to enable the United Nations to take urgent military measures, Members shall hold immediately available national air-force contingents for combined international enforcement action.
The strength and degree of readiness of these contingents and plans for their combined action shall be determined within the limits laid down in the special agreement or agreements referred to in Article 43, by the Security Council with the assistance of the Military Staff Committee.

Article 46

Plans for the application of armed force shall be made by the Security Council with the assistance of the Military Staff Committee.

Article 47

1. There shall be established a Military Staff Committee to advise and assist the Security Council on all questions relating to the Security Council's military requirements for the maintenance of international peace and security, the employment and command of forces placed at its disposal, the regulation of armaments, and possible disarmament.

2. The Military Staff Committee shall consist of the Chiefs of Staff of the permanent members of the Security Council or their representatives. Any Member of the United Nations not permanently represented on the Committee shall be invited by the Committee to be associated with it when the efficient discharge of the Committee's responsibilities requires the participation of that Member in its work.

3. The Military Staff Committee shall be responsible under the Security Council for the strategic direction of any armed forces placed at the disposal of the Security Council. Questions relating to the command of such forces shall be worked out subsequently.
4. The Military Staff Committee, with the authorization of the Security Council and after consultation with appropriate regional agencies, may establish regional sub-committees.

**Article 48**

1. The action required to carry out the decisions of the Security Council for the maintenance of international peace and security shall be taken by all the Members of the United Nations or by some of them, as the Security Council may determine.

2. Such decisions shall be carried out by the Members of the United Nations directly and through their action in the appropriate international agencies of which they are members.

**Article 49**

The Members of the United Nations shall join in affording mutual assistance in carrying out the measures decided upon by the Security Council.

**Article 50**

If preventive or enforcement measures against any state are taken by the Security Council, any other state, whether a Member of the United Nations or not, which finds itself confronted with special economic problems arising from the carrying out of those measures shall have the right to consult the Security Council with regard to a solution of those problems.

**Article 51**

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council
has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

CHAPTER VIII

REGIONAL ARRANGEMENTS

Article 52

1. Nothing in the present Charter precludes the existence of regional arrangements or agencies for dealing with such matters relating to the maintenance of international peace and security as are appropriate for regional action, provided that such arrangements or agencies and their activities are consistent with the Purposes and Principles of the United Nations.

2. The Members of the United Nations entering into such arrangements or constituting such agencies shall make every effort to achieve pacific settlement of local disputes through such regional arrangements or by such regional agencies before referring them to the Security Council.

3. The Security Council shall encourage the development of pacific settlement of local disputes through such regional arrangements or by such regional agencies either on the initiative of the states concerned or by reference from the Security Council.

4. This Article in no way impairs the application of Articles 34 and 35.
Article 53

1. The Security Council shall, where appropriate, utilize such regional arrangements or agencies for enforcement action under its authority. But no enforcement action shall be taken under regional arrangements or by regional agencies without the authorization of the Security Council, with the exception of measures against any enemy state, as defined in paragraph 2 of this Article, provided for pursuant to Article 107 or in regional arrangements directed against renewal of aggressive policy on the part of any such state, until such time as the Organization may, on request of the Governments concerned, be charged with the responsibility for preventing further aggression by such a state.

2. The term enemy state as used in paragraph 1 of this Article applies to any state which during the Second World War has been an enemy of any signatory of the present Charter.

Article 54

The Security Council shall at all times be kept fully informed of activities undertaken or in contemplation under regional arrangements or by regional agencies for the maintenance of international peace and security.

[Note: Chapters IX through XV are omitted]
CHAPTER XVI

MISCELLANEOUS PROVISIONS

Article 102

1. Every treaty and every international agreement entered into by any Member of the United Nations after the present Charter comes into force shall as soon as possible be registered with the Secretariat and published by it.

2. No party to any such treaty or international agreement which has not been registered in accordance with the provisions of paragraph 1 of this Article may invoke that treaty or agreement before any organ of the United Nations.

Article 103

In the event of a conflict between the obligations of the Members of the United Nations under the present Charter and their obligations under any other international agreement, their obligations under the present Charter shall prevail.

Article 104

The Organization shall enjoy in the territory of each of its Members such legal capacity as may be necessary for the exercise of its functions and the fulfilment of its purposes.

Article 105

1. The Organization shall enjoy in the territory of each of its Members such privileges and immunities as are necessary for the fulfilment of its purposes.
2. Representatives of the Members of the United Nations and officials of the Organization shall similarly enjoy such privileges and immunities as are necessary for the independent exercise of their functions in connexion with the Organization.

3. The General Assembly may make recommendations with a view to determining the details of the application of paragraphs 1 and 2 of this Article or may propose conventions to the Members of the United Nations for this purpose.

[Note: Chapters XVII through XIX are omitted]
DOCUMENT B

DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY


The General Assembly,

Recalling its resolutions on the role of science and technology in the context of international security in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of mankind’s creative potential, and for additional improvements in the circulation of information in the global community.
Recalling in this connection the approaches and principles outlined in the international Conference on the Information Society and Development, held in Midrand, South Africa, in 1996,

Taking note of the results of the Ministerial Conference devoted to the fight against terrorism held in Paris in July 1996 and of the recommendations it made,

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the security of States,

Considering that it is necessary to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes,

1. Calls upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;

2. Invites all Member States to inform the Secretary-General of their views and assessments of the following questions:

(a) General appreciation of the issues of information security;

(b) Definition of basic notions related to information security, including unauthorized interference with or
misuse of information and telecommunications systems and information resources;

(c) Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help combat information terrorism and criminality;

3. Requests the Secretary-General to submit a report to the General Assembly at its fifty-fourth session;

4. Decides to include in the provisional agenda of its fifty-fourth session the item entitled “Developments in the field of information and telecommunications in the context of international security.”

Mr. Chairman,

The United States joined in adoption by consensus of the draft resolution entitled, “Developments in the field of information and telecommunications in the context of international security” (L.17/Rev.1). We commend the flexibility shown by the main sponsor in pursuing this initiative. We believe the text just adopted outlines a balanced approach that will enable the international community to begin thoughtful and reflective consideration of this new and complicated topic.

The General Assembly’s adoption of the resolution in plenary will launch the international community on a complex enterprise encompassing many interrelated factors which delegates to the First Committee do not ordinarily address. For example, the topic includes technical aspects that relate to global communications – as well as non-technical issues associated with economic cooperation and trade, intellectual property rights, law enforcement, anti-terrorist cooperation, and other issues that are considered in the Second or Sixth Committee. Further, the actions and programs of governments are by no means the only appropriate focus, for the initiative also involves important
Mr. Chairman, the United States believes it will be important for the international community’s future consideration of this topic to draw on the experience of delegates to the Second and Sixth Committees. We believe it will be at least equally important to seek ideas and insights from a broad range of experts in our respective governments and societies.

Thank you, Mr. Chairman.
DOCUMENT D

HAGUE DECLARATION IV, 1

Declaration (IV, 1), to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons, and Other Methods of Similar Nature, July 29, 1899, *reprinted in The Laws of Armed Conflicts* 201, 202-05 (Dietrich Schindler & Jiri Toman eds., 3d ed. 1988). The author gratefully acknowledges the availability of the electronic version of this document located at www.icrc.org which was provided by the International Committee of the Red Cross.

The undersigned, Plenipotentiaries of the Powers represented at the International Peace Conference at The Hague, duly authorized to that effect by their Governments, inspired by the sentiments which found expression in the Declaration of St. Petersburg of 29 November (11 December) 1868,

Declare that:

The Contracting Powers agree to prohibit, for a term of five years, the launching of projectiles and explosives from balloons, or by other new methods of a similar nature.

The present Declaration is only binding on the Contracting Powers in case of war between two or more of them.

It shall cease to be binding from the time when, in a war between the Contracting Powers, one of the belligerents is joined by a non-Contracting Power.

The present Declaration shall be ratified as soon as possible.
The ratifications shall be deposited at The Hague.

A *procès-verbal* shall be drawn up on the receipt of each ratification, of which a copy, duly certified, shall be sent through the diplomatic channel, to all the Contracting Powers.

The non-Signatory Powers may adhere to the present Declaration. For this purpose they must make their adhesion known to the Contracting Powers by means of a written notification addressed to the Netherlands Government, and communicated by it to all the other Contracting Powers.

In the event of one of the High Contracting Parties denouncing the present Declaration, such denunciation shall not take effect until a year after the notification made in writing to the Netherlands Government, and by it forthwith communicated to all the other Contracting Powers.

This denunciation shall only affect the notifying Power.

In faith of which the Plenipotentiaries have signed the present Declaration, and affixed their seals thereto.

Done at The Hague, 29 July 1899, in a single copy, which shall be kept in the archives of the Netherlands Government, and of which copies, duly certified, shall be sent through the diplomatic channel to the Contracting Powers.

(Here follow signatures)
DOCUMENT E

HAGUE DECLARATION XIV

Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons, Oct.18, 1907, reprinted in THE LAWS OF ARMED CONFLICTS 201, 202-06 (Dietrich Schindler & Jiri Toman eds., 3d ed. 1988). The author gratefully acknowledges the availability of the electronic version of this document located at www.icrc.org which was provided by the International Committee of the Red Cross.

The undersigned, Plenipotentiaries of the Powers invited to the Second International Peace Conference at The Hague, duly authorized to that effect by their Governments, inspired by the sentiments which found expression in the Declaration of St. Petersburg of 29 November (11 December) 1868, and being desirous of renewing the declaration of The Hague of 29 July 1899, which has now expired,

Declare:

The Contracting Powers agree to prohibit, for a period extending to the close of the Third Peace Conference, the discharge of projectiles and explosives from balloons or by other new methods of a similar nature.

The present Declaration is only binding on the Contracting Powers in case of war between two or more of them.

It shall cease to be binding from the time when, in a war between the Contracting Powers, one of the belligerents is joined by a non-Contracting Power.
The present Declaration shall be ratified as soon as possible.

The ratifications shall be deposited at The Hague. A procès-verbal shall be drawn up recording the receipt of the ratifications, of which a duly certified copy shall be sent, through the diplomatic channel, to all the Contracting Powers.

Non-Signatory Powers may adhere to the present Declaration. To do so, they must make known their adhesion to the Contracting Powers by means of a written notification, addressed to the Netherlands Government, and communicated by it to all the other Contracting Powers.

In the event of one of the High Contracting Parties denouncing the present Declaration, such denunciation shall not take effect until a year after the notification made in writing to the Netherlands Government, and forthwith communicated by it to all the other Contracting Powers.

This denunciation shall only have effect in regard to the notifying Power.

In faith whereof the Plenipotentiaries have appended their signatures to the present Declaration.

Done at The Hague, 18 October 1907 in a single copy, which shall remain deposited in the archives of the Netherlands Government, and duly certified copies of which shall be sent through the diplomatic channel, to the Contracting Powers.

(Here follow signatures)
Computers and computer-dependent systems permeate everyone’s daily life. From local, state, and federal government decision makers to warfighters, businessmen, lawyers, doctors, bankers, and individuals – everyone relies upon information and information systems that involve the acquisition, transmission, storage, or transformation of information. For as little as five or ten dollars a month, anyone with a computer has access to instantaneous world-wide communications and a wealth of resources on the internet. Instead of human watch standers, computerized sensing and control devices now monitor transportation, oil, gas, electrical, and water treatment systems throughout our Nation. Satellites serve as the backbone of our telecommunication systems and our economic well being. The Global Positioning System (GPS) guides virtually all of the commercial aircraft in the world.

The Department of Defense is heavily dependent upon timely and accurate information, and is keenly focused on information operations and information assurance. Military commanders in Bosnia receive real-time satellite imagery. Marine warfighters are training on Wall Street to learn how to respond
during information-intense situations; Navy commanders are focusing on network centric warfare; Army planners believe the use of a tactical internet will have profound implications for battle tactics; and Air Force information warriors now have their own squadron. Over 95% of Department of Defense telecommunications travel over commercial systems, and the interdependence of our civilian infrastructure and national security grows dramatically on a daily basis. In a few short decades, the global networking of computers via the internet will very likely be viewed as the one invention that had the greatest impact on human civilization – and perhaps the greatest challenge to our national security.

All of these computers and computer-dependent systems are vulnerable to physical and electronic attack – from the computers on which individuals store and process classified information, privileged attorney-client information, or proprietary data, to our nationwide telecommunication and banking systems. Indeed, the year 2000 problem demonstrates that we are even vulnerable to our own misfeasance and poor planning. A single non-nuclear, electromagnetic pulse can destroy or degrade circuit boards and chips, or erase all electronic media on Wall Street, in the Pentagon, or your local bank. The loss of a single satellite can terminate service for over 90% of the 45 million pagers in the United States, as well as interrupt service for thousands of cable television stations and credit card transactions. GPS signals can be spoofed or degraded, or used as part of highly accurate targeting systems. Advanced computer technology can help build nuclear weapons. Internet and computer crime is so simple that two teenagers in Cloverdale, California with a mentor in Israel can break into sensitive national security systems at the Department of Defense. Information warfare experts can use global television to selectively influence political and economic decisions or produce epileptic-like spasms in viewers. Cyber warfare of the 21st century
could significantly impact the daily lives of every man, woman, and child in America.

**DEVELOPING ECONOMIC POTENTIAL**

Although the telephone was invented in 1876, the personal computer in 1975, and the internet in the 1970’s, the world wide web, as we know it today, was not invented until 1991. By the year 2002, Americans will spend nearly $38 billion online annually. The enormous economic potential of the world wide web was quickly recognized by the U.S. Government.

On 15 September 1993, President Clinton established the “United States Advisory Council on the National Information Infrastructure” by Executive Order 12864. This Advisory Council was tasked to advise the Secretary of Commerce on a national strategy and other matters related to the development of the National Information Infrastructure (NII). The final report of the Advisory Council was transmitted to the President on 30 January 1996. The Council’s report, “A Nation of Opportunity: Realizing the Promise of the Information Superhighway” (available at GPO) made a series of detailed recommendations that addressed four issues: reducing legal, regulatory, and policy barriers on the key areas of American life and work that will be impacted by the NII; gaining universal access to the NII for all; developing rules of the road regarding intellectual property, privacy, and security on the NII; and identifying the roles of the key stakeholders in developing the NII.

On 1 July 1997, President Clinton approved another report entitled “A Framework for Global Electronic Commerce.” This report set forth the Administration’s vision of the emerging global electronic market-place with minimal regulation and no discriminatory taxes and tariffs. In developing our economic potential, however, we also increase our vulnerabilities.
IDENTIFYING NATIONAL SECURITY VULNERABILITIES

As the United States Government studied the tremendous economic potential of the internet, it began to realize the significant national security vulnerabilities inherent in our reliance on computers and computer-dependent systems. On 15 July 1996, President Clinton signed Executive Order 13010, establishing the “President’s Commission on Critical Infrastructure Protection” (CIP). This Commission was the first national effort to address the vulnerabilities created by the new information age.

Executive Order 13010 declared that certain “national infrastructures are so vital that their incapacity or destruction [by either physical or cyber attack] would have a debilitating impact on the defense or economic security of the United States.” The Executive Order detailed eight categories of critical infrastructures: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and continuity of government. The President acknowledged in the text of the Executive Order that because so many of these critical infrastructures are owned and operated by the private sector, “it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.”

The President’s Commission was chaired by retired Air Force General Robert T. Marsh, and was comprised of members of the federal government and industry. Its work was guided by a Steering Committee of senior government officials and an Advisory Committee of key industry leaders. The Commission was tasked to develop a comprehensive national strategy for protecting critical infrastructures from physical and electronic threats. Because threats to our Nation’s critical infrastructure were
considered very real, the Executive Order also established an “Infrastructure Protection Task Force” (IPTF) as an interim coordinating measure. The IPTF was created within the Department of Justice to increase the “coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact.”

A hundred-page unclassified version of its report entitled “Critical Foundations: Protecting America’s Infrastructures” was released on 13 October 1997. The President’s Commission found no evidence of an “impending cyber attack which could have a debilitating effect on the Nation’s critical infrastructures.” It did, however, find a widespread capability to exploit our infrastructure vulnerabilities that is real, and growing at an alarming rate for which we have little defense. The Commission also identified potential threats that included insiders, recreational and institutional hackers, organized criminals, industrial competitors, terrorists, and states. Because our Nation’s critical infrastructures are mainly privately owned and operated, the Commission concluded that “critical infrastructure assurance is a shared responsibility of the public and private sectors,” and the only sure way to protect infrastructures is through a real partnership between infrastructure owners and the government.

The Commission made a series of seven findings. First, information sharing is the most immediate need. Second, responsibility is shared among owners and operators and the government. Third, infrastructure protection requires integrated capabilities of diverse federal agencies, and special means for coordinating federal response to ensure these capabilities are melded together effectively. Fourth, the challenge is one of adapting to a changing culture. Fifth, the federal government has important roles in the new infrastructure protection alliance with industry and state and local governments. Sixth, the existing legal
framework is imperfectly attuned to deal with cyber threats. Seventh, research and development are not presently adequate to support infrastructure protection. To prepare a policy framework for its recommendations, the Commission also adopted seven principles: build on that which exists; depend on voluntary cooperation; start with the owners and operators; practice continuous improvement; coordinate security with maintenance and upgrades; promote government leadership by example; and minimize changes to government oversight and regulation. The Commission’s recommendations addressed what actions it believed the federal government should take, what actions industry should take, and what actions that government and industry must take in partnership.

Key to the Commission’s national strategy is the international and domestic legal regime required to protect against cyber threats. The objective of the Commission’s legal initiatives was to sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts. Eighteen specific recommendations were made by the Commission that were intended to strengthen existing legal frameworks for federal response to and deterrence of incidents and the adequacy of criminal law and procedure, as well as to change those laws that inhibit protective efforts and information sharing.

The report of the President’s Commission has been criticized by some in government and industry for not providing complete or detailed solutions to our infrastructure vulnerabilities after fifteen months of work. It is, however, an extraordinary effort that gives our national leadership a recommended conceptual and organizational framework to analyze, manage, and defend against the threats to our critical infrastructure. It is also the template upon which the President has designed his plan for critical infrastructure protection.
DEFENDING OUR CRITICAL INFRASTRUCTURE

On 22 May 1998, President Clinton issued two Presidential Decision Directives (PDD) that will build the interagency framework to strengthen and coordinate our critical infrastructure defense programs. PDD 62, *Combating Terrorism*, is the broader of the two directives and focuses on the growing threat of all unconventional attacks against the United States such as terrorist acts, use of weapons of mass destruction, assaults on critical infrastructures, and cyber attacks. It establishes the position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. Richard Clarke has been appointed to fill this National Security Council position, which is intended to bring a more systematic, program management approach to counter-terrorism, protection of critical infrastructure, preparedness, and consequence management. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs.

PDD 63, *Critical Infrastructure Protection*, builds upon the recommendations set forth in the report of the President’s Commission on Critical Infrastructure Protection. It calls for immediate action by the federal government and a national effort between government and industry to swiftly assure the continuity and viability of our critical infrastructures. The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism designated pursuant to PDD 62 is responsible for coordinating the implementation of PDD 63. The President’s first, and perhaps most important, of ten principles set forth to guide the interagency in addressing and eliminating potential vulnerabilities is for those involved to consult with and seek input from Congress on approaches and programs to meet the objectives of PDD 63.
President Clinton has declared in PDD 63 a national goal of significantly increased security for government systems by the year 2000 and a reliable, interconnected, and secure information system infrastructure by the year 2003. To achieve this goal, PDD 63 organizes the federal government around four components: lead agencies for sector liaison, lead agencies for special functions, an interagency working group for critical infrastructure protection coordination, and a National Infrastructure Assurance Council. Unlike most Presidential decision directives which focuses only on government organization and interagency coordination, PDD 63 is remarkable in its efforts to mobilize a public-private partnership to reduce critical infrastructure vulnerability.

For each of the eight major sectors of our economy that are vulnerable to infrastructure attack, a single U.S. Government department is designated to serve as the lead agency for liaison to cooperate with the private sector. These sector liaisons will coordinate with private sector representatives to address problems related to critical infrastructure protection, to develop a sector component of the National Infrastructure Assurance Plan, and to develop and implement a Vulnerability Awareness and Education Program for their sector. By way of example, the Department of Commerce is the lead agency for the information and communications sectors, and the Department of Treasury is the lead agency for the banking and finance sectors.

A National Plan Coordination (NPC) staff will integrate these sector component plans into the comprehensive National Infrastructure Assurance Plan and coordinate the analyses of the U.S. Government’s own dependencies on critical infrastructure. PDD 63 specifies that the NPC shall be an office of the Department of Commerce beginning fiscal year 1999. On 22 May 1998, the Secretary of Commerce named Jeffrey Hunker, formerly Deputy Assistant to the Secretary of Commerce for economic policy development and special initiatives, as Director of the
national Critical Infrastructure Assurance Office (CIAO). The Director of the CIAO will report to the PDD 62 National Coordinator and will be responsible for the duties assigned by PDD 63 to the NPC staff.

Similarly, for each of the functions that must be chiefly performed by the federal government, four lead agencies for special functions have been designated. The Department of Justice is the lead agency for law enforcement and internal security, the Central Intelligence Agency is the lead agency for foreign intelligence, the Department of State is the lead agency for foreign affairs, and the Department of Defense is the lead agency for national defense. The departmental representatives from these twelve lead agencies, as well as representatives from other relevant departments and agencies, will meet to coordinate the implementation of PDD 63 under the auspices of the Critical Infrastructure Coordination Group (CICG), which will be chaired by the PDD 62 National Coordinator.

The National Infrastructure Assurance Council will consist of a panel of major infrastructure providers and state and local government officials. Its purpose is to enhance the partnership of the public and private sectors, and it is authorized to make reports to the President as it believes appropriate. The Chairman of the Council will be appointed from industry, and the PDD 62 National Coordinator will serve as the Council’s executive director.

Every department and agency of the federal government is responsible for protecting its own critical infrastructure, and must develop a plan to do so within 180 days of 22 May 1998, the issuance of PDD 63. The PDD 62 National Coordinator is responsible for coordinating the analyses required by the departments and agencies, and the CICG will sponsor an expert review process for those plans. These plans must be fully implemented no later than 22 May 2000, and are suppose to serve
as a model to the private sector on how best to protect critical infrastructure. Also within 180 days of 22 May, the Principals Committee must submit to the President a schedule for completing the National Infrastructure Assurance Plan.

PDD 63 also authorizes the Federal Bureau of Investigation to continue the operation of its National Infrastructure Protection Center (NIPC) to provide a national focal point for gathering information on threats to critical infrastructures. The NIPC will serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. It will also provide the principal means of facilitating and coordinating the federal government’s response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. If the threat is identified as foreign, then the President may place the NIPC in a direct support role to either the Department of Defense or the Intelligence Community. The NIPC was created on 27 February 1998, and Michael Vatis was appointed to serve as its chief.

Finally, PDD 63 encourages the owners and operators of the critical infrastructures to create a private sector Information Sharing and Analysis Center (ISAC). The design of the ISAC, and its relationship to the NIPC, was left to the determination of the private sector, however, the PDD 63 National Coordinator is required to identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

IMPLICATIONS FOR THE LEGAL COMMUNITY

The implications for the legal community are profound. In many respects, international and domestic law has been overwhelmed by a revolution in technology that is driving an unparalleled evolution in national security and online commercial
law which involves individuals and industry as well as state, local, and federal governments at all levels.

During the 20th century, Americans have felt safe at home from foreign attack, and armed conflict has historically been the province of the federal government and the military industrial complex. Wars were fought elsewhere because the United States has the ability to project its great military power overseas and protect American soil from attack. Our economy has thrived and computer technology has flourished. As the United States became the world’s greatest military and economic power, its computer-dependent infrastructure also became the world’s most vulnerable and lucrative target. Our military and economic strength forces those who wish to do us harm to attack our soft underbelly – the computer and computer-dependent systems throughout our Nation that were initially built with an open architecture and without security foremost in mind. This soft underbelly that supports a war effort may have always been a lawful target under the laws of armed conflict, but without today’s internet technology, enemy states could not reach these targets on American soil. Today, however, hostile states can easily target America’s heartland with a $900 computer and techniques readily available on the internet. Given that over 95% of Department of Defense telecommunications travel over commercial systems, and the growing interdependence of our civilian infrastructure and national security complex, lawyers must evaluate whether the rules of military necessity and collateral damage under existing laws of war, *jus in bello*, are adequate in the information age.

National security lawyers must also try to define what is a use of force in cyberspace. An unauthorized intrusion by individuals or terrorists into a national security system is criminal activity under the jurisdiction of the Department of Justice. In contrast, the same type of intrusion by a state, or a state sponsored individual or terrorist, may be lawful espionage or intelligence
gathering under international law, or it may be an unlawful use of force under the Charter of the United Nations by a state that gives rise to another state’s inherent right of self-defense. Lawyers must define when a state’s activity in another state’s national security computer system becomes a hostile act, or a demonstration of hostile intent, that authorizes either an electronic or a conventional, steel-on-target response in self-defense. The law of conflict management, *jus ad bellum*, must be reviewed and refined to prevent future conflict.

Lawyers throughout state, local, and federal governments must review existing legislation, and propose new legislation as necessary, to ensure that the United States has a coordinated approach toward the prevention, mitigation, response, recovery, and reconstitution of damage to our critical infrastructure. Department of Justice lawyers and prosecutors in all fifty states must initiate legislative changes that will strengthen our ability to investigate, prosecute, and deter computer crime. Multinational mutual legal assistance treaties are needed to enhance international cooperation and eliminate safe havens that may exist around the world. While we strengthen these laws, we must also ensure that we protect the privacy rights of all consumers and operators, and that we do not restrict an online free market by over regulation. We must also ensure that all existing and new laws clearly provide procedures for government and industry to test their own computer systems without fear of violating international or domestic law, and authority for the federal government to conduct intelligence collection and information operations to defend our Nation.

Lawyers are also challenged with the new application of commercial law to online and electronic storage applications. Liability for the buying and selling of goods and services online raises many issues involving online contracts, digital signatures, and electronic payments. Internet provider liability issues based on theories of direct infringement, contributory infringement, and
vicarious liability abound because of the ease with which copyright protected works can be duplicated and distributed on the internet. The trend in the courts appear to limit the liability of internet service providers (ISPs) for content based liability in defamation suits, but ISPs must be careful about the nature of their service contracts with publishers to ensure they keep their distance from an editorial role that may give rise to liability.

Business lawyers and trial attorneys must consider the trustworthiness and admissibility of electronic records and emails in an online world. Corporate lawyers must be concerned about the liability of their principals and board of directors for failing to maintain legally acceptable standards of care in protecting their computers and information systems from theft, data manipulation, or destruction. Lawyers for insurance companies should be proactive and develop standards of care and security practices that are prerequisites to coverage. Intellectual property lawyers must be concerned about the unauthorized and misleading use of similar domain names and universal resource locators (URLs). Civil rights lawyers must address online First Amendment issues raised in recent legislation attempting to protect children from sexually explicit materials and predators, and privacy issues that arise when employers track internet usage and electronic communications of their employees.

A resolution to the national debate over encryption will have significant ramifications for law enforcement and private industry – in the meantime, international travelers must be careful carrying some common software packages that contain sophisticated encryption packages because United States law may prohibit their export, and import should you return, from the United States without an export control license. Depending upon the jurisdiction where they practice, lawyers must be concerned about breaching their ethical duty of confidentiality when sending electronic mail over the internet. They must also be aware of
issues that involve the unauthorized practice of law that may arise when advising clients with a multistate presence. Similarly, lawyers who have a federal practice such as immigration law that market over the internet must be concerned about the unauthorized practice of law when they advise clients in another state via email. Lawyers who advertise on the web must also be concerned about unethical advertising issues in some states when using key words that suggest specialties. The new national security and online commercial law issues that are evolving have the potential to touch every lawyer, regardless if they are in government service or private practice – and the burden is on the entire legal profession to help create a plan that will protect our critical infrastructure while protecting individual and business rights in cyberspace.

ANALYSIS AND CONCLUSION

The President’s Commission on Critical Infrastructure Protection concluded that our vulnerability to cyber attack by criminals, terrorists, and hostile states is real and growing. The Commission’s report provided a series of detailed recommendations that would provide a strategy to defend our critical infrastructures. PDD 63 embraces the Commission’s report by establishing a public-private partnership, and the structure within the federal government to lead industry by example as to how best to protect our critical infrastructure. The President has demonstrated by his actions and PDD 63 his commitment to working with the private sector and Congress.

In fact, Congress deserves as much of the credit as any government agency or office for identifying the vulnerabilities of our infrastructure and shaping the solution we now see in PDD 63. Many of the initiatives and conclusions of the Commission’s report and PDD 63 were shaped and influenced, if not originated, by legislation and Congressional hearings. Without the leadership and initiative of Senator Jon Kyl, Congressman Porter Goss, and
Congressman Curt Weldon, to name only three who have been actively involved, the United States would be much further from developing a plan to protect our Nation’s critical infrastructure.

Two of the most difficult issues facing the United States concerns information sharing and encryption. Information must flow both ways between the government and private industry to ensure the United States has an effective early warning mechanism against an organized cyber attack. Private industry must have encryption to ensure the integrity of electronic transactions, and United States companies must have the economic and competitive advantage by being able to enter the international market. Encryption will also help make our critical infrastructure more secure. Law enforcement and intelligence agencies, however, have a legitimate need to be able to conduct electronic surveillance in the age of sophisticated digital encryption. Within very carefully crafted constitutional, statutory, and regulatory safeguards and procedures, both the law enforcement and intelligence communities already have the right to conduct electronic surveillance as a matter of law under appropriate circumstances – but with the technology of digital encryption, they will not have the technical capability to do so without a system in place that allows them access to a key.

Unfortunately, the principal reason why there is not yet a solution for either the information sharing or encryption issue is the lack of trust that private industry has in the government. There has also been disagreement as to who will bear the cost to private industry of implementation. The solutions will not be easy. What is clear, however, is that both the government and private industry have competing equities in developing a solution to each of these issues, and that both government and private industry will have to compromise to reach a solution. What is also clear, is that not having a solution to the information sharing issue leaves critical infrastructures more vulnerable, and not having a solution to the
encryption issue places American businesses at an economic and competitive disadvantage.

Just as with the report of the President’s Commission, many people in government and industry will, undoubtedly, criticize and find what they view as faults with PDD 63. Indeed, it is not perfect, and perhaps never intended to be. As always, hindsight and experience will likely prove there was a better approach. The report of the President’s Commission and PDD 63 are, however, extraordinary accomplishments. Together, they have given us the ability to grasp an extremely complex problem and have given us a plan for action that assigns relatively clear responsibilities within the government. If the government is able to maintain its momentum created by the President’s Commission on Critical Infrastructure Protection, PDD 63 should be able to move the Executive, Congress, and private sector forward in partnership to define the National Infrastructure Assurance Plan that will effectively protect our great Nation’s critical infrastructure in this new era of national security.
DOCUMENT G

DEFINITION OF AGGRESSION


The General Assembly,

Having considered the report of the Special Committee on the Question of Defining Aggression, established pursuant to its resolution 2330 (XXII) of 18 December 1967, covering the work of its seventh session held from 11 March to 12 April 1974, including the draft Definition of Aggression adopted by the Special Committee by consensus and recommended for adoption by the General Assembly,

Deeply convinced that the adoption of the Definition of Aggression would contribute to the strengthening of international peace and security,

1. Approves the Definition of Aggression, the text of which is annexed to the present resolution;

2. Expresses its appreciation to the Special Committee on the Question of Defining Aggression for its work which resulted in the elaboration of the Definition of Aggression;

3. Calls upon all States to refrain from all acts of aggression and other uses of force contrary to the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations;
4. Calls the attention of the Security Council to the Definition of Aggression, as set out below, and recommends that it should, as appropriate, take account of that Definition as guidance in determining, in accordance with the Charter, the existence of an act of aggression.

2319th plenary meeting
14 December 1974

ANNEX
Definition of Aggression

The General Assembly,

Basing itself on the fact that one of the fundamental purposes of the United Nations is to maintain international peace and security and to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace,

Recalling that the Security Council, in accordance with Article 39 of the Charter of the United Nations, shall determine the existence of any threat to the peace, breach of the peace or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security,

Recalling also the duty of States under the Charter to settle their international disputes by peaceful means in order not to endanger international peace, security and justice,

Bearing in mind that nothing in this Definition shall be interpreted as in any way affecting the scope of the provisions of
the Charter with respect to the functions and powers of the organs of the United Nations,

*Considering also* that, since aggression is the most serious and dangerous form of the illegal use of force, being fraught, in the conditions created by the existence of all types of weapons of mass destruction, with the possible threat of a world conflict and all its catastrophic consequences, aggression should be defined at the present stage,

*Reaffirming* the duty of States not to use armed force to deprive peoples of their right to self-determination, freedom and independence, or to disrupt territorial integrity,

*Reaffirming also* that the territory of a State shall not be violated by being the object, even temporarily, of military occupation or of other measures of force taken by another State in contravention of the Charter, and that it shall not be the object of acquisition by another State resulting from such measures or the threat thereof,

*Reaffirming also* the provisions of the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations,

*Convinced* that the adoption of a definition of aggression ought to have the effect of deterring a potential aggressor, would simplify the determination of acts of aggression and the implementation of measures to suppress them and would also facilitate the protection of the rights and lawful interests of, and the rendering of assistance to, the victim,

*Believing* that, although the question whether an act of aggression has been committed must be considered in the light of
all the circumstances of each particular case, it is nevertheless desirable to formulate basic principles as guidance for such determination,

Adopts the following Definition of Aggression:

Article 1

Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition.

Explanatory note: In this Definition the term “State”:

(a) Is used without prejudice to questions of recognition or to whether a State is a member of the United Nations;

(b) Includes the concept of a “group of States” where appropriate.

Article 2

The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity.
Article 3

Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression:

(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;

(b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;

(c) The blockade of the ports or coasts of a State by the armed forces of another State;

(d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;

(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;

(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed
force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

Article 4

The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter.

Article 5

1. No consideration of whatever nature, whether political, economic, military or otherwise, may serve as a justification for aggression.

2. A war of aggression is a crime against international peace. Aggression gives rise to international responsibility.

3. No territorial acquisition or special advantage resulting from aggression is or shall be recognized as lawful.

Article 6

Nothing in this Definition shall be construed as in any way enlarging or diminishing the scope of the Charter, including its provisions concerning cases in which the use of force is lawful.

Article 7

Nothing in this Definition, and in particular article 3, could in any way prejudice the right to self-determination, freedom and independence, as derived from the Charter, of peoples forcibly deprived of that right and referred to in the Declaration on Principles of International Law concerning Friendly Relations and Co-operations among States in accordance with the Charter of the
United Nations, particularly peoples under colonial and racist regimes or other forms of alien domination; nor the right of these peoples to struggle to that end and to seek and receive support, in accordance with the principles of the Charter and in conformity with the above-mentioned Declaration.

**Article 8**

In their interpretation and application the above provisions are interrelated and each provision should be construed in the context of the other provisions.
ENCLOSURE A
STANDING RULES OF ENGAGEMENT FOR US FORCES

1. Purpose and Scope

a. The purpose of these SROE is to provide implementation guidance on the inherent right and obligation of self-defense and the application of force for mission accomplishment. The SROE establish fundamental policies and procedures governing the actions to be taken by US force commanders during all military operations, contingencies, or prolonged conflicts. In order to provide uniform training and planning capabilities, this document is authorized for distribution to commanders at levels to be used as fundamental guidance for training and directing their forces.

b. Except as augmented by supplemental ROE for specific operations, missions, or projects, the policies and procedures established herein remain in effect until rescinded.
c. US forces operating with multinational forces:

(1) US forces assigned to the OPCON [operational control] of a multinational force will follow the ROE of the multinational force unless otherwise directed by the NCA [National Command Authorities]. US forces will be assigned and remain OPCON to a multinational force only if the combatant commander and higher authority determine that the ROE for that multinational force are consistent with the policy guidance on unit self-defense and with the rules for individual self-defense contained in this document.

(2) When US forces, under US OPCON, operate in conjunction with a multinational force, reasonable efforts will be made to effect common ROE. If such ROE cannot be established, US forces will exercise the right and obligation of self-defense contained in this document while seeking guidance from the appropriate combatant command. To avoid mutual interference, the multinational forces will be informed prior to US participation in the operation of the US forces’ intentions to operate under these SROE and to exercise unit self-defense. For additional guidance concerning peace operations, see Appendix A to Enclosure A.

(3) Participation in multinational operations may be complicated by varying national obligations derived from international agreements; i.e., other members in a coalition may not be signatories to treaties that bind the United States, or they may be bound by treaties to which the United States is not a party. US forces still remain bound by US treaty obligations even if the other members in a
coalition are not signatories to a treaty and need not adhere to its terms.

d. Commanders of US forces subject to international agreements governing their presence in foreign countries (e.g., Status of Forces Agreements) are not relieved of the inherent authority and obligation to use all necessary means available and to take all appropriate action for unit self-defense.

e. US forces in support of operations not under operational or tactical control of a combatant commander or performing missions under direct control of the NCA, Military Departments, or other US government departments/agencies (i.e., marine security guards, certain special security forces) will operate under use-of-force policies or ROE promulgated by those departments or agencies.

f. US Coast Guard (USCG) units and units under USCG OPCON conducting law enforcement operations, and USCG personnel using their law enforcement authority, will follow the use-of-force policy issued by the Commandant, USCG. Nothing in the USCG use-of-force policy negates a commander’s inherent authority and obligation to use all necessary means available and to take all appropriate action for unit self-defense in accordance with these SROE.

g. The guidance in this document does not cover US forces deployed to assist federal and local authorities during times of civil disturbance within the territorial jurisdiction of any state, the District of Columbia, Commonwealths of Puerto Rico and the Northern Marianas, US possessions, and US territories. Forces in these situations will follow use-of-force policy found in DOD Civil Disturbance Plan, “Garden Plot” (Appendix 1 to Annex C of Garden Plot).
h. US forces deployed to assist foreign, federal, and local authorities in disaster assistance missions, such as earthquakes and hurricanes, will follow use-of-force guidelines as set forth in the mission’s execute order and subsequent orders.

i. US forces will always comply with the Law of Armed Conflict. However, not all situations involving the use of force are armed conflicts under international law. Those approving operational rules of engagement must determine if the internationally recognized Law of Armed Conflict applies. In those circumstances when armed conflict, under international law, does not exist, Law of Armed Conflict principles may nevertheless be applied as a matter of national policy. If armed conflict occurs, the actions of US forces will be governed by both the Law of Armed Conflict and rules of engagement.

2. Policy

a. THESE RULES DO NOT LIMIT A COMMANDER’S INHERENT AUTHORITY AND OBLIGATION TO USE ALL NECESSARY MEANS AVAILABLE AND TO TAKE ALL APPROPRIATE ACTION IN SELF-DEFENSE OF THE COMMANDER’S UNIT AND OTHER US FORCES IN THE VICINITY.

b. US national security policy serves to protect the United States, US forces, and, in certain circumstances, US citizens and their property, US commercial assets, and other designated non-US forces, foreign nationals, and their property from hostile attack. US national security policy is guided, in part, by the need to maintain a stable international environment compatible with US national security interests. In addition, US national security interests guide our global objectives of deterring armed attack against the United States across the range of military operations, defeating an attack should
deterrence fail, and preventing or neutralizing hostile efforts to intimidate or coerce the United States by the threat or use of armed force or terrorist actions. Deterrence requires clear and evident capability and resolve to fight at any level of conflict and, if necessary, to increase deterrent force capabilities and posture deliberately so that any potential aggressor will assess its own risks as unacceptable. US policy, should deterrence fail, provides flexibility to respond to crises with options that:

(1) Are proportional to the provocation.

(2) Are designed to limit the scope and intensity of the conflict.

(3) Will discourage escalation.

(4) Will achieve political and military objectives

3. **Intent.** These SROE are intended to:

   a. Provide general guidelines on self-defense and are applicable worldwide to all echelons of command.

   b. Provide guidance governing the use of force consistent with mission accomplishment.

   c. Be used in operations other than war, during transition from peacetime to armed conflict or war, and during armed conflict in the absence of superseding guidance.

4. **Combatant Commanders’ SROE**

   a. Combatant commanders may augment these SROE as necessary to reflect changing political and military policies, threats, and missions specific to their AOR [Area of
Responsibility]. When specific standing rules governing the use of force in a combatant commander’s AOR are required that are different from these SROE, they will be submitted to the Chairman of the Joint Chiefs of Staff for NCA approval as necessary and promulgated by the Joint Staff as an Annex to Enclosure C of these SROE.

b. Combatant commanders will distribute these SROE to subordinate commanders and units for compliance. The mechanism for disseminating ROE supplemental measures is set forth in Enclosure B.

5. Definitions

a. **Inherent Right of Self-Defense.** A commander has the authority and obligation to use all necessary means available and to take all appropriate action to defend that commander’s unit and other US forces in the vicinity from a hostile act or demonstrated hostile intent. Neither these rules, nor the supplemental measures activated to augment these rules, limit this inherent right and obligation. At all times, however, the requirements of necessity and proportionality as amplified in these SROE will be the basis for the judgment of the commander as to what constitutes an appropriate response to a particular hostile act or demonstration of hostile intent.

b. **National Self-Defense.** National self-defense is the act of defending the United States, US forces, and in certain circumstances, US citizens and their property, US commercial assets, and other designated non-US forces, foreign nationals and their property, from a hostile act or hostile intent. Once a force or terrorist unit is declared hostile by appropriate authority exercising the right and obligation of national self-defense (see paragraph 2 of Appendix A to Enclosure A),
individual US units do not need to observe a hostile act or determine hostile intent before engaging that force.

NOTE: **Collective Self-Defense.** Collective self-defense, as a subset of national self-defense, is the act of defending other designated non-US forces, personnel and their property from a hostile act or demonstration of hostile intent. Only the NCA may authorize US forces to exercise collective self-defense.

c. **Unit Self-Defense.** Unit self-defense is the act of defending a particular unit of US forces, including elements or personnel thereof, and other US forces in the vicinity, against a hostile act or hostile intent. The need to exercise unit self-defense may arise in many situations such as localized low-level conflicts, humanitarian efforts, peace enforcement actions, terrorist response, or prolonged engagements. Individual self-defense is a subset of unit self-defense; see the glossary for a definition of individual self-defense.

d. **Elements of Self-Defense.** The application of armed force in self-defense requires the following two elements:

   (1) **Necessity.** A hostile act occurs or a force or terrorist unit exhibits hostile intent.

   (2) **Proportionality.** The force used must be reasonable in intensity, duration, and magnitude, based on all facts known to the commander at the time, to decisively counter the hostile act or hostile intent and to ensure the continued safety of US forces.

e. **Hostile Act.** A hostile act is an attack or other use of force by a foreign force or terrorist unit (organization or individual) against the United States, US forces, and in certain
circumstances, US citizens, their property, US commercial assets, and other designated non-US forces, foreign nationals and their property. It is also force used directly to preclude or impede the mission and/or duties of US forces, including the recovery of US personnel and vital US Government property. When a hostile act is in progress, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. (See definitions in the Glossary for amplification.)

f. **Hostile Intent**. Hostile intent is the threat of imminent use of force by a foreign force or terrorist unit (organization or individual) against the United States, US forces, and in certain circumstances, US citizens, their property, US commercial assets, or other designated non-US forces, foreign nationals and their property. When hostile intent is present, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat. (See definitions in the Glossary for amplification.)

g. **Hostile Force**. Any force or terrorist unit (civilian, paramilitary, or military), with or without national designation, that has committed a hostile act, demonstrated hostile intent, or has been declared hostile.

6. **Declaring Forces Hostile**. Once a force is declared hostile by appropriate authority, US units need not observe a hostile act or a demonstration of hostile intent before engaging that force. The responsibility for exercising the right and obligation of national self-defense and declaring a force hostile is a matter of the utmost importance demanding considerable judgment of command. All available intelligence, the status of international relationships, the requirements of international law, the possible need for a political
decision, and the potential consequences for the United States must be carefully weighed. Exercising the right and obligation of national self-defense by competent authority is in addition to and does not supplant the right and obligation to exercise unit self-defense. The authority to declare a force hostile is limited as amplified in Appendix A to Enclosure A.

7. Authority to Exercise Self-Defense
   a. **National Self-Defense.** The authority to exercise national self-defense is outlined in Appendix A to Enclosure A.
   b. **Collective Self-Defense.** Only the NCA may authorize the exercise of collective self-defense.
   c. **Unit Self-Defense.** A unit commander has the authority and obligation to use all necessary means available and to take all appropriate action to defend the unit, including elements and personnel thereof, or other US forces in the vicinity, against a hostile act or hostile intent. In defending against a hostile act or hostile intent under these SROE, unit commanders should use only that degree of force necessary to decisively counter the hostile act or hostile intent and to ensure the continued safety of US forces.

8. Action in Self-Defense
   a. **Means of Self-Defense.** All necessary means available and all appropriate actions may be used in self-defense. The following guidelines apply for unit or national self-defense:
      (1) **Attempt to Control Without the Use of Force.** The use of force is normally a measure of last resort. When time and circumstances permit, the potentially hostile force should be warned and given the opportunity to withdraw or
cease threatening actions. (See Appendix A to Enclosure A for amplification.)

(2) **Use Proportional Force To Control the Situation.** When the use of force in self-defense is necessary, the nature, duration, and scope of the engagement should not exceed that which is required to decisively counter the hostile act or hostile intent and to ensure the continued safety of US forces or other protected personnel or property.

(3) **Attack To Disable or Destroy.** An attack to disable or destroy a hostile force is authorized when such action is the only prudent means by which a hostile act or hostile intent can be prevented or terminated. When such conditions exist, engagement is authorized only until the hostile force no longer poses an imminent threat.

b. **Immediate Pursuit of Hostile Foreign Forces.** In self-defense, US forces may pursue and engage a hostile force that has committed a hostile act or demonstrated hostile intent and that remains an imminent threat. (See Appendix A to Enclosure A for amplification.)

c. **Defending US Citizens, Property, and Designated Foreign Nationals**

   (1) **Within a Foreign Nation’s US Recognized Territory or Territorial Airspace.** A foreign nation has the principal responsibility for defending US citizens and property within these areas. (See Appendix A to Enclosure A for amplification.)

   (2) **At Sea.** Detailed guidance is contained in Annex A to Appendix B of this enclosure.
(3) **In International Airspace.** Protecting civil aircraft in international airspace is principally the responsibility of the nation of registry. Guidance for certain cases of actual or suspected hijacking of airborne US or foreign civil aircraft is contained in MCM-102-92, 24 July 1992, “Hijacking of Civil Aircraft.”

(4) **Terrorism.** Terrorist attacks are usually undertaken by civilian or paramilitary organizations, or by individuals under circumstances in which a determination of hostile intent may be difficult. The definitions of hostile act and hostile intent set forth above will be used in situations where terrorist attacks are likely. The term “hostile force” includes terrorist units when used in this document. When circumstances and intelligence dictate, supplemental ROE will be used to meet this special threat.

(5) **Piracy.** Piracy is defined as an illegal act of violence, depredation (i.e., plundering, robbing, or pillaging), or detention in or over international waters committed for private ends by the crew or passengers of a private ship or aircraft against another ship or aircraft or against persons or property on board such ship or aircraft. US warships and aircraft have an obligation to repress piracy on or over international waters directed against any vessel, or aircraft, whether US or foreign flagged. If a pirate vessel or aircraft fleeing from pursuit proceeds into the territorial sea, archipelagic waters, or superjacent airspace of another country every effort should be made to obtain the consent of nation sovereignty to continue pursuit. Where circumstances permit, commanders will seek guidance from higher authority before using armed force to repress an act of piracy.
d. **Operations Within or in the Vicinity of Hostile Fire or Combat Zones Not Involving the United States**

(1) US forces should not enter, or remain in, a zone in which hostilities (not involving the United States) are imminent or occurring between foreign forces unless directed by proper authority.

(2) If a force commits a hostile act or demonstrates hostile intent against US forces in a hostile fire or combat zone, the commander is obligated to act in unit self-defense in accordance with SROE guidelines.

e. **Right of Assistance Entry**

(1) Ships, or under certain circumstances aircraft, have the right to enter a foreign territorial sea or archipelagic waters and corresponding airspace without the permission of the coastal or island state to engage in legitimate efforts to render emergency assistance to those in danger or distress from perils of the sea.

(2) Right of assistance extends only to rescues where the location of those in danger is reasonably well known. It does not extend to entering the territorial sea, archipelagic waters, or national airspace to conduct a search.

(3) For ships and aircraft rendering assistance on scene, the right and obligation of self-defense extends to and includes persons, vessels, or aircraft being assisted. The right of self-defense in such circumstances does not include interference with legitimate law enforcement actions of a coastal nation. However, once received on board the assisting ship or aircraft, persons assisted will not
be surrendered to foreign authority unless directed by the NCA.

(4) Further guidance for the exercise of the right of assistance entry is contained in CJCS Instruction 2410.01, 20 July 1993, "Guidance for the Exercise of Right of Assistance Entry."
**INDEX**

<table>
<thead>
<tr>
<th>Term</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggression, Definition of:</td>
<td>33 n.85, 114, 116, 211</td>
</tr>
<tr>
<td>Aggressive use of force:</td>
<td>33 n.85, 33-36, 82, 104, 136-37, 145</td>
</tr>
<tr>
<td>Armed attack</td>
<td>Application of existing law: 81-119</td>
</tr>
<tr>
<td></td>
<td>Computer espionage: 129, 131</td>
</tr>
<tr>
<td></td>
<td>Computer network attack: 132-34</td>
</tr>
<tr>
<td></td>
<td>Defined: 119, 145</td>
</tr>
<tr>
<td></td>
<td>Introduction to: 6-7, 11-14</td>
</tr>
<tr>
<td></td>
<td>Military applications: 25</td>
</tr>
<tr>
<td></td>
<td>Relation to Common Art. 2: 58-69</td>
</tr>
<tr>
<td></td>
<td>Scope, duration, and intensity: 76-77, 80</td>
</tr>
<tr>
<td></td>
<td>Under <em>jus ad bellum</em>: 36-37, 43-48, 51, 54</td>
</tr>
<tr>
<td>Armed conflict</td>
<td>Defined: 13, 59, 145</td>
</tr>
<tr>
<td>Armed force</td>
<td>Defined: 145</td>
</tr>
<tr>
<td>Charter of the United Nations</td>
<td>As contemporary <em>jus ad bellum</em>: 33-54</td>
</tr>
<tr>
<td>Civil affairs (CA)</td>
<td>24, 146</td>
</tr>
<tr>
<td>CJCSI 3121.01:</td>
<td>95 n.237, 219</td>
</tr>
<tr>
<td>CJCSI 3210.01A:</td>
<td>141 n.325</td>
</tr>
<tr>
<td>Common Article 2</td>
<td>Evolution: 55-58</td>
</tr>
<tr>
<td></td>
<td>Defining an armed attack: 58-67</td>
</tr>
<tr>
<td></td>
<td>Generally: 55-69</td>
</tr>
<tr>
<td>Communications intelligence (COMINT):</td>
<td>124, 146</td>
</tr>
<tr>
<td>Computer espionage</td>
<td>Defined: 146</td>
</tr>
<tr>
<td></td>
<td>Generally: 123-32</td>
</tr>
<tr>
<td>Computer network attack (CNA)</td>
<td>Defined: 146</td>
</tr>
<tr>
<td></td>
<td>Generally: 132-33</td>
</tr>
<tr>
<td>Covert operation</td>
<td>111 n.289, 147</td>
</tr>
<tr>
<td>Critical infrastructure protection:</td>
<td>195-210</td>
</tr>
<tr>
<td>CyberSpace</td>
<td>Application of international law: 1-14</td>
</tr>
<tr>
<td></td>
<td>Defined: 15, 147</td>
</tr>
<tr>
<td></td>
<td>Military applications: 15-25</td>
</tr>
<tr>
<td>De facto hostilities:</td>
<td>59-67</td>
</tr>
<tr>
<td>Electronics intelligence (ELINT):</td>
<td>124, 147</td>
</tr>
<tr>
<td>Electronic warfare (EW):</td>
<td>23, 147</td>
</tr>
<tr>
<td>Espionage</td>
<td>Defined: 148</td>
</tr>
<tr>
<td></td>
<td>Generally: 123-32</td>
</tr>
<tr>
<td>Executive Order 13010:</td>
<td>22, 131, 198</td>
</tr>
<tr>
<td>Foreign instrumentation signals intelligence (FISINT):</td>
<td>125, 148</td>
</tr>
<tr>
<td>Hague Declaration (IV, 1):</td>
<td>2 n.4, 191</td>
</tr>
<tr>
<td>Hague Declaration (XIV):</td>
<td>2 n.5, 193</td>
</tr>
<tr>
<td>Hostile act:</td>
<td>61, 94-95, 99, 132, 135, 149, 206, 224-226</td>
</tr>
<tr>
<td>Hostile intent:</td>
<td>14, 94-96, 99, 101, 130-35, 140, 149, 206</td>
</tr>
<tr>
<td>Imagery intelligence (IMINT):</td>
<td>125, 149</td>
</tr>
<tr>
<td>Information operations (IO):</td>
<td>23-24, 125, 140-41, 150, 195, 206</td>
</tr>
<tr>
<td>Information warfare (IW):</td>
<td>24, 150, 196</td>
</tr>
<tr>
<td>International Court of Justice (ICJ):</td>
<td>48, 71, 81, 100, 109, 111, 150</td>
</tr>
<tr>
<td>International Committee of the Red Cross:</td>
<td>56, 191, 193</td>
</tr>
<tr>
<td>International law</td>
<td>Application in CyberSpace: 1-14</td>
</tr>
<tr>
<td></td>
<td>Categories relevant to use of force: 6-7</td>
</tr>
<tr>
<td></td>
<td>Sources of: 71-72</td>
</tr>
<tr>
<td></td>
<td>Violations of: 97-101</td>
</tr>
<tr>
<td>Internet</td>
<td>10, 12, 15-17, 19-25, 42, 86-87, 102-03, 108-09, 112, 117-18, 127, 150</td>
</tr>
<tr>
<td>Joint Pub 1-02:</td>
<td>24 n.48, 111 n.289</td>
</tr>
<tr>
<td>Joint Pub 3-07:</td>
<td>65 n.176</td>
</tr>
<tr>
<td>Joint Pub 3-13:</td>
<td>24 n.45, 125 n.311</td>
</tr>
<tr>
<td></td>
<td>Armed attack: 36-37, 43-48, 51, 54</td>
</tr>
<tr>
<td></td>
<td>Collateral damage and injury to civilians: 40-43</td>
</tr>
<tr>
<td></td>
<td>Contemporary: 33-54</td>
</tr>
<tr>
<td></td>
<td>Defined: 28, 151</td>
</tr>
<tr>
<td></td>
<td>Economic force: 88-93</td>
</tr>
<tr>
<td></td>
<td>Evolution: 27-32</td>
</tr>
<tr>
<td></td>
<td>Indirect armed force: 110-13</td>
</tr>
<tr>
<td></td>
<td>Necessity and proportionality: 37-40</td>
</tr>
<tr>
<td></td>
<td>Obligation to settle: 83-87</td>
</tr>
<tr>
<td></td>
<td>Political force: 88-93</td>
</tr>
<tr>
<td></td>
<td>Protection of nationals abroad: 104-10</td>
</tr>
<tr>
<td></td>
<td>Self-defense and the use of force: 37-49, 154</td>
</tr>
<tr>
<td></td>
<td>Security Council authority: 49-52</td>
</tr>
<tr>
<td></td>
<td>Threats of force: 93-97</td>
</tr>
<tr>
<td></td>
<td>Unarmed, non-military physical force: 101-103</td>
</tr>
<tr>
<td></td>
<td>Violations of international law: 97-101</td>
</tr>
</tbody>
</table>
### Index

**Jus in bello**
- Application to LOCM: 55-58
- Defined: 55, 151

**Law of armed conflict (LOAC):** 7, 39, 55-60, 151

**Law of conflict management (LOCM):** 7, 27-54, 151

**Law of information conflict (LOIC):** 11, 151

**Law of War:** 55, 151

**Line of belligerency:** 9, 67-68, 152

**Military applications of CyberSpace:** 15-25

**Military deception:** 23, 152

**Nicaragua v. United States:** 48 & n.132, 82 n.197

**Occupation:** 58 & n.153, 67, 69, 96, 115, 138, 152, 215

**Open-source intelligence (OSINT):** 127, 152

**Operations security (OPSEC):** 23, 152

**Psychological operation (PSYOP):** 23, 153

**Public affairs (PA):** 24, 153

**Reprisal:** 85 & n.214, 91, 153

**Retortion:** 85 & n.214, 153

**Rules of engagement (ROE):** 94, 128, 153

**Scope, duration, and intensity test:** 7, 60-69, 75-77, 80, 95, 100, 103, 108, 112, 117, 119, 133

**Self-defense:** 37-49, 154

**Shared understanding:** 64 & n.172

**Signals intelligence (SIGINT):** 124, 154

**Standing Rules of Engagement (SROE):** 94, 95 & n.237, 154, 219

**Threats of the use of force:** 93-97

**Use of force:** 118, 155

**United Nations**
- See Charter of the United Nations
- G.A. Res. 2625: 111 n.285
- G.A. Res. 3314: 114 n.295, 211
- G.A. Res. 53/70: 1 n.1, 5 n.12, 185
- Explanation of vote: 6 n.13, 189

**War:** 13, 24, 27-32, 39-42, 57-60, 155

**World Wide Web (WWW):** 12, 15-19, 155
CYBERSPACE AND THE USE OF FORCE focuses specifically on one of the most challenging, contentious, and important issues in international law: how to determine what constitutes a use of force between states in Cyberspace under the contemporary UN Charter paradigm of conflict management. Though referenced in detail for lawyers, this text provides the necessary legal background to make it a useful desk reference for government officials, military operators, students, and others who are interested in the application of international law in Cyberspace.

A National Security Law in Cyberspace Book
ISBN: 0-9670326-0-1

Aegis Research Corporation is a leading provider of world class expertise in information operations (policy, strategy, and analysis), information security, threat analysis, threat characterization and countermeasures, mission planning and simulation, security implementation support, comprehensive enterprise strategy development, enterprise protection planning, and professional technical services for the federal national security community, state and local governments, and U.S. corporations.

Aegis Research Corporation
We enable information advantage.™