OXFORD

Cyber Operations and the Use of Force in International Law

Marco Roscini

Marco Roscini

CONTENTS

Chapter 2: Cyber operations and the *ius ad bellum*

I. Introduction

II. Cyber operations and the prohibition of the threat and use of force in international relations

1. Cyber operations as a 'use of force'

1.1 Cyber attacks causing physical damage to property, loss of life or injury to persons

1.2 Cyber attacks severely disrupting critical infrastructures

1.3 Cyber attacks below the level of the use of force

1.4 Cyber exploitation

1.5 Activities related to cyber operations

2. Cyber operations and threats of force

III. Cyber operations and the law of self-defence

1. Cyber operations as 'armed attack'

2. Anticipatory self-defence against an imminent cyber armed attack

3. Self-defence against cyber attacks by non-state actors

4. Necessity, proportionality and immediacy of the reaction in self-defence

5. Collective self-defence in reaction to a cyber armed attack: the cases of NATO and the European Union

6. The standard of evidence required for the exercise of self-defence against cyber armed attacks

7. The duty to report the self-defence measures to the UN Security Council

IV. Remedies against cyber operations short of armed attack

V. Chapter VII of the United Nations Charter and the role of the Security Council

VI. Conclusions.

Chapter 3: The applicability of the *ius in bello* to cyber operations

I. Introduction

II. Cyber operations in and as international armed conflicts

1. Declared war

2. Cyber operations 'in the context of' an existing international armed conflict

3. Cyber operations without concurrent kinetic hostilities

3.1 'resort to armed force'

3.1.1 'Use of force' and 'resort to armed force'

3.1.2 Does the 'resort to armed force' need to reach a minimum level of intensity to initiate an international armed conflict?

3.2 'between states'

III. Cyber operations during partial or total belligerent occupation

IV. Cyber operations in and as non-international armed conflicts

1. Article 3 Common to the 1949 Geneva Conventions

1.1 'protracted' armed violence

1.2 The organization requirement

2. Additional Protocol II

V. Cyber operations as ‘internal disturbances and tensions’

VI. Conclusions.

Chapter 4: Cyber operations and the conduct of hostilities

I. Introduction

II. The legality of means and methods of cyber warfare

III. The law of targeting

1. The obligation to direct attacks exclusively against military objectives

1.1 When does a cyber operation amount to an ‘attack’?

1.2 The definition of ‘military objective’

a) ‘effective contribution to military action’

b) ‘definite military advantage’

c) Is the internet a military objective?

1.3 Targetable individuals

a) Members of a belligerent state’s regular armed forces, including members of militias or volunteer corps forming part of such armed forces

b) Members of other militias and volunteer corps belonging to a belligerent state

c) Members of the armed forces of a non-state actor

d) Civilians taking direct part in (cyber) hostilities

e) Civilians accompanying the armed forces

f) Civil defence personnel

g) Levée en masse

1.4 Are there geographical limitations to attacks on combatants and on civilians conducting cyber operations that amount to direct participation in hostilities?

1.5 Ruses of war and the prohibition of perfidy

2. The prohibition of indiscriminate attacks

2.1 The principle of proportionality

3. Objects and persons specially protected from attack

4. The duty to take precautions

4.1 Precautions in attack

4.2 Precautions against the effects of an attack

IV. Cyber operations short of 'attack' and the law on the conduct of hostilities

V. Cyber operations as remedies against violations of the law of armed conflict

VI. Conclusions

Chapter 5: Cyber operations and the law of neutrality

I. Introduction

II. When does the law of neutrality apply?

III. The law of neutrality and its consequences on the conduct of cyber operations

1. Cyber operations from neutral territory