

# Contents

|  |      |
|--|------|
| <i>List of figures</i>   | ix   |
| <i>List of tables</i>  | x    |
| <i>List of text boxes</i>  | xi   |
| <i>List of abbreviations</i>   | xiii |
| <i>Acknowledgments</i>   | xv   |
| <i>Preface to the second edition</i>   | xvii |
| 1 Introduction   | 1    |
| 2 The technological foundations of insecurity in the digital age                     | 11   |
| 3 Cyberspace and international relations   | 36   |
| 4 Exploit: from signals intelligence to cyber warriors                               | 63   |
| 5 Attack: from exploitation to offensive cyber operations                            | 81   |
| 6 Shape: subvert, deceive, poison  | 98   |
| 7 The topology and history of major cyber conflict episodes                          | 111  |
| 8 National experiences with cybersecurity: realization and institutional development | 147  |
| 9 States at cyberwar: the dynamics and national strategies of cyber conflict         | 186  |
| 10 Cyber conflict as “grey zone” conflict  | 220  |
| 11 Non-state actors: terrorism, subversion and activism online                       | 240  |

|   |     |
|---|-----|
| 12 Norms, ethics and international law for offensive cyber operations | 273 |
| 13 Evolution: how the logics of cyber conflict might change           | 300 |
| 14 Revolution: how the nature of cyber conflict might change          | 315 |

|                 |     |
|-----------------|-----|
| <i>Glossary</i> | 322 |
| <i>Index</i>    | 333 |

|   |     |
|---|-----|
| 1 Introduction  | 1   |
| 2 The technological foundations of asymmetric warfare in the digital age            | 11  |
| 3 Cyberspace and international relations  | 39  |
| 4 Exploit from signal intelligence to cyber espionage                               | 69  |
| 5 Attacks from exploitation to offensive cyber operations                           | 81  |
| 6 Snake, subvert, deceive, poison   | 109 |
| 7 The topology and history of major cyber conflict episodes                         | 141 |
| 8 National experiences with cyberattacks: legislation and institutional development | 167 |
| 9 States as cyberswar: the dynamics and national strategies of cyber conflict       | 181 |
| 10 Cyber conflict as "grey zone" conflict   | 230 |
| 11 Non-state actors: terrorism, subversion and activism online                      | 240 |