



Mohamed Amer

Former EUCOM Country Desk Officer
and Cyber Policy Advisor

In the wake of a world forever reshaped by the Ukraine War, 'Defending The Future' materializes as the ultimate roadmap to strengthening global cyber resilience and fortifying our interconnected digital world. This riveting narrative uncovers the grave intersections of cyber defense, security cooperation, and global stability in the boisterous aftermath of one of our most momentous geopolitical events.

In 'Defending The Future', readers embark on a journey into the intricacies of U.S. cyberspace security cooperation and observe the unfolding evolution of international cyber capacity building. The book unearths the threads of intention, the ominous perceptions of rising tensions, and the ever-growing capacity for cyber warfare in a digitally interconnected world.

With a keen eye on the past and a vision for the future, this book employs insightful analysis and foresight to unravel the complexities of cyberspace conflict. As the realm of digital threats continues to expand, it offers an indispensable guide for crafting robust strategies and cooperative security pacts and alliances, equipping the United States, its Allies and partners, governments, and organizations with the knowledge and tools needed to secure our shared digital future.

A must-read for policymakers, foreign service & desk officers, cybersecurity practitioners, and anyone intrigued by the interplay of geopolitics, global security, and technology. 'Defending The Future' presents a compelling narrative that educates and inspires.

Step into a future where collaborative cyber defense is paramount, and integrated deterrence is the key to safeguarding our democracy in the U.S. and beyond. The future awaits, and it's time to defend it.

'Defending The Future' is your guide to navigating the complex landscape of cyberspace security cooperation in a post-Ukraine War era.



DEFENDING THE FUTURE

MOHAMED AMER



DEFENDING THE FUTURE

ADVANCING U.S. CYBERSPACE
SECURITY COOPERATION IN THE
POST-UKRAINE WAR ERA

MOHAMED AMER

**Defending the Future:
Advancing
U.S. Cyberspace Security
Cooperation in the
Post-Ukraine War Era**



www.defending-the-future.com

MOHAMED AMER

Disclaimer

The views expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the Department of Defense or the U.S. government. The public release clearance of this publication by the Department of Defense does not imply the Department of Defense endorsement or factual accuracy of the material.

DEFENDING THE FUTURE

Copyright © 2024 NY Publishers

First Edition

www.defending-the-future.com

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review.

Printed by NY Publishers in the USA.

nypublishers.co

Table of Contents

Disclaimer	ii
Dedication	xxv
About The Author	xxvii
Preface	xxix
Chapter 1: Capacity Building Investment in the Context of the Current International Order in Cyberspace.....	1
Introduction	1
Protecting the Public Core of the Internet.....	2
Geopolitical Shifts and Undersea Cables.....	3
Fostering Internet Security Initiatives and Investments to Mitigate Disruptions	5
Securing Electoral Infrastructure and Public Confidence	6
Ransomware Attacks and the 2022 US Elections	7
The Role of Non-State Actors	8
Ransomware Attacks and Non-State Actors	11
Protecting State Critical Infrastructure.....	13
Ransomware Attacks and Critical Infrastructure	15
The Adoption of Protective Measures	17
The Fight Against Ransomware.....	17
Whole of Government (WoG) Approach.....	19

Embracing the UK's 'Early Warning' Defense	20
Cyber Capacity Building Investment Needs.....	23
Conclusion.....	25
Chapter 2: Assessing the Trends of Conflict in Cyberspace: A Glimpse into 2023 and Beyond	27
Introduction	27
Intentions: A Push for Transparency in Offensive Cyber Capabilities	27
Perceptions: Escalating Interstate Tensions in Cyberspace.....	28
Capacity: Cyber Military Spending and National Cybersecurity	30
Activity: Cyber-Enabled Espionage, Attacks, and Disinformation Campaigns	32
Global Ransomware Attacks in 2022-2023	35
Visualizing the Trends: A Comparative Analysis.....	36
Forecasting Ransomware Attacks for 2023-2024.....	37
Conclusion.....	39
Chapter 3: Navigating Hybrid Conflict: Strategies for Cyberspace Security Cooperation	40
Introduction	40
Increasing Perception and Use of Hybrid Warfare	40
Growing Capability to Engage in Hybrid Conflict.....	42

Rising Military Activity	44
Political Interference on the Rise.....	47
Economic Coercion as a Tool of Conflict.....	49
Information Warfare: The Rise of Disinformation Campaigns	51
Cyber Attacks on Critical Infrastructure	52
Visualizing Trends in Hybrid Conflict.....	55
Conclusion.....	57
Chapter 4: Introducing Integrated Deterrence in Cyberspace with Allies and Partners	58
Introduction	58
Integrated Deterrence: A Key Pillar of the 2022 National Defense Strategy (NDS)	59
Integrated Deterrence Framework.....	62
Strategic Integration: Developing a Common Understanding and Prioritization	63
Enhancing Integrated Deterrence in Cyberspace	67
Institutional Integration: Building Trust and Cooperation	68
The Importance of Institutional Integration in Information Sharing	69
Tactical Integration: Promoting Technology Transfer, Interoperability, and Shared Tactics	73

Emphasizing the Importance of Cybersecurity for Developing Nations.....	73
Boosting Morale and Resilience	74
Supporting Multinational Cyber Coalition Exercises	75
Enabling Tactical Integration with Allies and Partners	75
Conclusion.....	77
Chapter 5: Applying Integrated Deterrence with Allies and Partners in Cyberspace Security Cooperation	78
Introduction.....	78
Strategic Integration: A Shared Vision.....	79
Towards Cyber Unity: Fostering Strategic Alignment and Integration Among Allies.....	81
Institutional Integration: Sharing Information and Promoting Resiliency	82
Information Sharing at the Institutional Level Through Hunt Forward Operations (HFOs)	84
Tactical Integration: Strengthening Capabilities and Interoperability	85
From Tools to Tactics: Enhancing Cyber Defense Through Holistic Collaboration and Integration.....	85
Conclusion.....	88
Chapter 6: Developing A Combatant Command Campaign Plan (CCP) For Cyberspace Activities, Operations, And Investments (AOIs)	89

Introduction	89
The purpose of Combatant Command Campaign Plans (CCPs)	90
Understanding the Strategic Environment.....	97
Tabletop Exercise: Axis and Allies - European Area of Responsibility (AOR)	97
Task Analysis and Operational Design Development.....	101
Building the Command Campaign Plan (CCP)	102
Creating a Joint Scheme of Maneuver for Coordinated Cyber Operations in Theater	103
Coordinating Components: The Impact of CCP and TCO on Force Management.....	106
Conclusion.....	107
Chapter 7: Cyberspace Security Cooperation Platforms and Tools	108
Introduction	108
Socium Functionality	111
Socium Account Registration.....	112
Additional Cyberspace Security Cooperation Tools...112	
All Partners Access Network (APAN).....	112
Advana	113
Conclusion.....	113

Chapter 8: Country Plan, Cyber Line of Activity (LOA), and Cyber Engagement Plan	115
Introduction	115
Cyber LOA and Cyber Roadmap Explained	116
Cyberspace Operations LOA.....	117
The GCC J6 Role	118
Cyber Roadmap Purpose	119
Cyber Roadmap Goals and Objectives	119
Cyber Lines of Efforts	120
CFR Events (Activities/Meetings).....	120
Familiarization versus Training	121
CFR Event Planning.....	121
CFR Event Management.....	122
Conclusion.....	123
Chapter 9: Leveraging U.S. Fiscal Authorities and Investments for Enhanced Cyberspace Security Cooperation	124
Introduction	124
U.S. Funding Initiatives	125
Training with Friendly Foreign Countries (TWFFC).....	125
European Deterrence Initiative (EDI).....	125
How EDI Supports Cyberspace Security Cooperation.....	125

Wales Initiative Fund (WIF)	127
Traditional Combatant Commander Activities (TCA)	128
Scope and Types of Traditional Combatant Commander Activities	128
Expenses of United States Forces Only	129
Involvement of the Department of State	129
Ukraine Security Assistance Initiative (USAI)	130
U.S. Fiscal Authorities	131
10 U.S. Code § 321 - Training with Friendly Foreign Countries (TWICC): Payment of Training and Exercise Expenses.....	131
10 U.S. Code § 312 - Payment of Personnel Expenses Necessary for Theater Security Cooperation	134
NDAA FY16 §1251 - Training for Eastern European National Military Forces during Multilateral Exercises	134
10 U.S. Code §164 - Commanders of Combatant Commands: Assignment, Powers, and Duties	135
Conclusion.....	136
Chapter 10: From Policy to Practice: Exploring DOD's Title 10 and DOS's Title 22 in Cyberspace Security Cooperation	137
Introduction	137
Security Cooperation Policy and Objectives	137

Overview of Security Cooperation	138
Roles and Responsibilities in Security Cooperation ...	138
Congressional Role in Security Cooperation.....	139
Conclusion.....	140
Chapter 11: Security Cooperation Funding Options Under Title 22: Foreign Military Sales (FMS) and Foreign Military Financing (FMF)	141
Introduction.....	141
Countering Russian Influence Fund (CRIF).....	142
Counter China Influence Funds (CCIF).....	143
Case Study: Strengthening Cyberspace Security Cooperation through FMS and FMF in Montenegro.	144
Conclusion.....	147
Chapter 12: Strengthening Cyberspace Security Cooperation through Foreign Military Sales (FMS)	148
Introduction.....	148
The Foreign Military Sales (FMS) Program	148
The Role of FMS in Cyberspace Security Cooperation	149
Benefits of FMS in Strengthening Cyberspace Security Cooperation	149
FMS' Cybersecurity-Focused Use Cases	151

Use Case 1: FMS Cybersecurity Assistance Framework	151
Use Case 2: FMS Cybersecurity Training Program	153
Use Case 2: FMS Cyber Incident Response Center	154
Conclusion.....	154
Chapter 13: Foreign Military Sales Process and Case Development for Acquiring Cyber Capabilities for partner nations (PNs).....	155
Introduction	155
Initiation and Assessment.....	156
Partner Engagement and Capability Identification ...	156
FMS Case Development and Agreement	157
Technical Assessment and Customization	159
Training and Capacity Building	159
Integration and Deployment	159
Monitoring and Continuous Improvement.....	160
Conclusion.....	160
Chapter 14: Security Cooperation Funding Options Under Title 10: Significant Security Cooperation Initiatives (SSCIs).....	161
Introduction	161
Significant Security Cooperation Initiatives (SSCIs) .	162
Conclusion.....	165

Chapter 15: Assessment, Monitoring, and Evaluation (AM&E) in Cyberspace Security Cooperation	167
Introduction	167
Initial Assessment.....	169
Initiative Design Document	170
Performance Management and Monitoring.....	172
Standards-based Evaluations in Security Cooperation Programs.....	173
Conclusion.....	174
Chapter 16: Leveraging Cyberspace Security Cooperation Maturity Model and Cybersecurity Focus Area Maturity Model in Capacity Building	176
Introduction.....	176
Joint Staff Cyberspace Security Cooperation Maturity Model (CSCM)	178
Level 0: Foundational Awareness.....	179
Level 1: Compliance-Driven Cybersecurity	179
Level 2: Risk-Driven Cybersecurity	180
Level 3: Common Defense	180
Level 4: Cyberspace Operations	181
Cybersecurity Focus Area Maturity (CYSFAM) Model	182

The Need for Cybersecurity Focus Area Maturity Model	182
The CYSFAM and Computer Incident Response Teams (CIRTs)	184
Assessing Cybersecurity Capabilities using CYSFAM	185
Conceptual Foundations of CYSFAM.....	185
Distinctive Characteristics of CYSFAM.....	186
Utilizing the CYSFAM model in Security Cooperation (SC) Activities.....	187
CYSFAM Artifact Development	187
Focus Area Example: Server Protection	193
CYSFAM Assessment Results.....	195
Future Improvements	197
Conclusion.....	197
Chapter 17: State Partnership Program (SPP).....	199
Introduction	199
Origins and Evolution of the State Partnership Program (SPP).....	199
Establishing State Partnerships: A Strategic Framework	201
Program Administration and Objectives.....	204

Military-to-Military Engagements and Defense Security Goals.....	204
Leveraging Whole-of-Society Relationships and Capabilities	205
Enduring Relationships	206
Statutory Authorities	206
Cost-Effectiveness and Value of the State Partnership Program	207
Conclusion.....	209
Chapter 18: The State Partnership Program (SPP): A Critical Component of Cyberspace Security Cooperation	212
Introduction.....	212
Special Capabilities of the SPP	212
Case 1: Cyber Defense Capacity Building in Ukraine	214
Case 2: Enhancing Cyber Resilience in the Baltic States	215
Case 3: Strengthening Cyber Defense Capabilities in Albania	215
Case 4: Promoting Cybersecurity Cooperation in Poland	216
Case 5: Building Cyber Defense Partnerships in Romania	216
Case 6: Strengthening Cyber Resilience in Bulgaria..	217

Case 7: Advancing Cybersecurity Cooperation in Montenegro.....	218
Case 8: Strengthening Cyber Resilience in North Macedonia.....	218
Case 9: Strengthening Cyber Defense Capabilities in Bosnia and Herzegovina	219
Case 10: Fostering Cybersecurity Cooperation in Kosovo	220
Conclusion.....	220
Chapter 19: The SPP in Focus: Examining Concerns and Strategies for Successful Cyberspace Security Cooperation	222
Introduction	222
Integration with Priorities of Combatant Commanders and Ambassadors	222
Civilian Engagements	223
Encroachment on DOS and USAID Responsibilities..	223
Future Strategies with the SPP	224
Conclusion.....	226
Chapter 20: Supporting Cyberspace Security Cooperation: PEO EIS's Defensive Cyber Operations (DCO) and the Allied Information Technology (AIT) Product Office....	227
Introduction	227
PEO EIS Mission and AIT Areas of Support.....	227

Establishment and Reputation Building.....	228
Comprehensive Service Delivery	228
Collaboration with Stakeholders	229
Data Utilization and Dashboard Development.....	229
Exploring Alternative Acquisition Strategies.....	229
Strategic Process and Mission Accomplishment	229
Conclusion.....	230
Chapter 21: Leveraging Defensive Cyber Operations (DCO) Capabilities and Platforms for Cyber Capacity Building.....	231
Introduction	231
Emerging Capabilities Platforms	232
Understanding Deployable and Garrison DCO Solutions in Cyber Defense	232
Deployable DCO System (DDS) in Focus: A Comprehensive Overview.....	233
Defensive Cyberspace Operations Tools Suite	236
Deployable DCO Solutions in the Modern Market.....	240
Conclusion.....	243
Chapter 22: Revolutionizing Defense Cyber Institutions Through Cybersecurity Skills and Training (CS&T) Platforms.....	244
Introduction	244

The Transformative Power of CS&T Platforms	245
Skill Demonstration and Potential Assessment	246
Comprehensive Skills and Gap Analysis	247
Customized Development Paths	247
Leveraging CS&T Platforms for Partner Nations	248
Key Advantages of CS&T Platforms	249
Implementing CS&T Platforms in Defense Cyber Institutions	250
Case Study: Leading CS&T Platforms	250
Conclusion.....	251
Chapter 23: Hunt Forward Operations and U.S. Cyberspace Security Cooperation	253
Introduction	253
HFOs' Defensive Nature.....	253
U.S. Cyber Forces and Command Authorities.....	255
Service Components.....	256
The Cyber Mission Force (CMF)	256
Cyber National Mission Force	257
Cyber Combat Mission Force	258
DODIN Operations and Defense	258
The Value of HFOs	258
Future HFOs and Expansion	261

Case Study: Unmasking Adversaries: HFOs as a Tool for Cyberspace Security Cooperation with Albania	262
Case Study: Defending Democracy: The Role of HFOs in Enhancing Cyberspace Security Cooperation with Montenegro.....	265
Case Study: Uniting Forces: The Birth of Cyber Command's Under Advisement Program for Enhanced Hunt Forward Operations (HFOs).....	267
Conclusion.....	270
Chapter 24: Advise & Assist (A&A) versus Hunt Forward Operations (HFOs) in Cyberspace Security Cooperation Activities.....	272
Introduction.....	272
Scope, Objectives, Engagement, and Collaboration ...	275
Authority Titles	279
Response Time During Cyber Crises	280
Conclusion.....	283
Chapter 25: The Bureau of Cyberspace and Digital Policy: Supporting Cyberspace Security Cooperation Objectives	285
Introduction	285
The mission of the Bureau.....	286
Conclusion.....	291

Chapter 26: Empowering Global Defense: The Role of Senior Cyber Advisors in Supporting Cyberspace Security Cooperation under the Global Defense Reform Program	292
Introduction	292
GDPR in Focus	292
Conclusion.....	298
Chapter 27: U.S. Cyberspace Security Cooperation and the Role of Multinational Cyber Exercises in the U.S. National Defense Strategy	300
Introduction	300
Benefits of Multinational Cyber Exercises	300
NATO Cyber Defence Pledge and its Impact on U.S. National Defense Strategy	302
Overview of Current Multinational DOD's Cyber Military Exercises	303
Building Multinational Cyber Exercises for Cyberspace Security Cooperation	305
Conclusion.....	306
Chapter 28: Harnessing Cyber Defense and CSIRT Assistance Programs for Cyberspace Security Cooperation with US Allies and Partners	307
Introduction	307
CSIRT Assistance Program (CAP) offered by Team Cymru	309

Benefits for U.S. Allies and Partners	309
Expanding Opportunities with Team Cymru	310
Leveraging the CAP and Additional Offerings: Practical Steps.....	311
CSIRT Assistance Program offered by CSIRT Global	312
The Cyber Defense Assistance Imperative (CDA).....	314
Defining Cyber Defense Assistance (CDA) and its Benefits	315
Challenges in Establishing Cyber Defense Assistance	315
The Cyber Defense Assistance Collaborative (CDAC) for Ukraine.....	315
The Future of Cyber Defense Assistance.....	316
Conclusion.....	317
Chapter 29: U.S. Cyberspace Security Cooperation and the Role of Multinational Cyber Exercises in the U.S. National Defense Strategy	318
Introduction	318
Benefits of Multinational Cyber Exercises	318
NATO Cyber Defence Pledge and its Impact on U.S. National Defense Strategy	320
Overview of Current Multinational DOD's Cyber Exercises.....	321
Building Multinational Cyber Exercises for Cyberspace Security Cooperation	322

Conclusion.....	324
Chapter 30: Rapid Response and International Cooperation: How the FBI's Cyber Action Team Assists U.S. Allies During Cyber Attacks	325
Introduction	325
The FBI's Cyber Action Team in Focus	325
The CAT's Mission and Expertise.....	325
Immediate Response and Implications of Cyber Attacks	326
Overseas Deployments and International Cooperation.....	326
Case Study 1: Iranian-sponsored Cyber Attack against Albania	327
Case Study 2: Russian-linked Cyber Attack against Montenegro.....	327
Conclusion.....	328
Chapter 31: Beyond Security: Cyber Capacity's Impact on Global Development.....	329
Introduction	329
Establishing a Common Language for Cyber Capacity Building	329
Addressing Diverse Challenges in Capacity Building	330
Divergent Priorities in Cyber Capacity Building.....	332
Tailoring Solutions: One Size Does Not Fit All	333

The Role of National Cybersecurity Strategies	335
International Coordination in Cyber Capacity Building	335
Stakeholders' Cooperation in Cyber Capacity Building	336
Addressing Challenges in Incident Reporting.....	337
Essential Elements for Success.....	339
Elevating the Priority of Cyber Capacity Building.....	341
Transitioning from Needs to Delivery	343
Conclusion.....	344
APPENDIX A: Sample Cyber Engagement Form.....	347
APPENDIX B: Sample CRIF Proposal	348
APPENDIX C: Performance-based Site Survey Assessment Template	352
APPENDIX D – CYSFAM Model Assessment Questions	365
APPENDIX E: National Guard State Partnership Program Map.....	387
APPENDIX F: Lexicon Of Cyberspace Security Cooperation Terms and Related Definitions	388
APPENDIX G: U.S. Security Cooperation Organizations Guide	395
APPENDIX H: Cyberspace SC Abbreviations List.....	412

Bibliography418

Dedication

To my family,

This book is dedicated to the unwavering support and love you have shown me throughout my life. Your encouragement and belief in my dreams have been the driving force behind my journey, and I am eternally grateful for everything you have done for me.

As an immigrant and first-generation American, I carried with me the dreams I had since I was a young boy. Growing up, I aspired to become a G.I. Joe, “America’s fighting man,” who wanted to make the world a better place. Little did I know that my path would indeed lead me to become just that.

My journey has been filled with challenges and adversity in both my military and civilian career. However, your support and unwavering belief in me have been my constant source of strength. You taught me the values of hard work, perseverance, and the importance of making a difference in the world.

This book is a testament to my efforts to make the world a better place despite the obstacles that stood in my way. It is a reflection of the sacrifices you made and the sacrifices we endured as a family. It is a tribute to the resilience and determination that runs in our blood, passed down through generations.

MOHAMED AMER

Thank you for standing by me, for believing in my dreams, and for being the foundation upon which I built my life. This book is as much yours as it is mine, and I hope it serves as a reminder that with love, support, and determination, we can overcome anything life throws our way.

With all my love and gratitude,

Mohamed Amer.



DEFENDING THE FUTURE

About The Author

Mohamed Amer is a Cyber Capacity Building SME with over twenty years of experience in cyber strategy, defensive cyber operations (DCO), and military intelligence (MI), as well as security cooperation (SC) and assistance as it relates to cyberspace. Mohamed possesses extensive expertise, spanning fifteen years, in various cyber security domains within the U.S. Department of Defense (DOD) and Intelligence Community (IC). His areas of specialization include cyberspace security cooperation, indications and warnings, threat hunting, incident response, risk assessment, penetration testing, intrusion detection, and malware forensics. Mohamed served as a Cyberspace Security Cooperation Advisor to the U.S. European Command (USEUCOM or EUCOM) in Germany.ⁱ He has experience working closely with foreign Ministries of Defense and Cyber Commands, U.S. Embassies, and Country Team leadership to ensure security cooperation objectives are met. As a Cyberspace Security Cooperation Advisor to the U.S. European Command, Mohamed was part of the first USEUCOM-led cyber exercise, Cyber Unity, dedicated to Military CISRTS of NATO Allies, sponsored by Luxembourg's Directorate of Defence and NATO Support and Procurement Agency (NSPA).ⁱⁱ

Prior to his EUCOM role, Mohamed spent eight years supporting the U.S. Army Europe and Africa (USAREUR-AF) and U.S. Army Cyber Command (ARCYBER). In addition, for six years, Mohamed served as a cyber threat and intelligence Analyst in the U.S. Army at the Cyber Battalion at Fort Eisenhower in Georgia. Mohamed holds a Master of Science

degree (MSc) in Information Assurance and Security from Western Governors University in Utah.

In his free time, Mohamed develops open-source software to protect non-profit organizations from ransomware attacks through an anti-ransomware detection tool designed to search and identify phishing campaigns and legitimate MITRE ATT&CK tools that are hard to detect. The open-source scanner also scrutinizes foreign-made software and highlights its impact on organizations' security posture.ⁱⁱⁱ

Preface

Welcome to “Defending The Future: Advancing U.S. Cyberspace Security Cooperation in the Post-Ukraine War Era.” This book is an essential resource born out of a pressing need in the market for comprehensive guides and references on cyberspace security cooperation. Its aim is to fill the gap and provide practitioners with a valuable tool for navigating the complexities of this field.

One of the primary motivations behind writing this book is the lack of available resources and practical guides that specifically address the intricacies of cyberspace security cooperation within U.S. foreign policy. As cyber threats continue to evolve and intensify, the importance of collaboration across borders has become paramount. Yet, there has been a dearth of comprehensive guidance for newcomers and even seasoned practitioners with limited cyber experience. This book endeavors to be the first of its kind, incorporating everything one needs to know about U.S. cyberspace security cooperation, making it accessible to individuals from diverse backgrounds.

Within the pages of this book, we cover a wide range of topics critical to understanding and effectively engaging in cyberspace security cooperation. We explore the concept of integrated deterrence in cyberspace, examine the strategies and techniques of Advise & Assist (A&A), and delve into the complexities of Hunt Forward Operations (HFOs). Additionally, we address key aspects such as DOD's Title 10 and DoS's Title 22, cyberspace security cooperation force providers and stakeholders, Foreign Military Sales (FMS),

Foreign Military Financing (FMF), Computer Security Incident Response Team (CSIRT) Assistance Programs, and the FBI Cyber Action Team (CAT), as well as Significant Security Cooperation Initiatives (SSCIs) Assessment, Monitoring, and Evaluation (AM&E) activities. By encompassing these essential elements, this resource aims to equip readers with a comprehensive understanding and practical guide of the field.

The book caters to two distinct audiences: newcomers entering the field of cyberspace security cooperation and experienced policymakers and practitioners. For those new to the field, we provide a solid foundation by explaining fundamental concepts, terminologies, and challenges in the cyberspace domain. Our goal is to demystify complex technical jargon and make the core principles of cyberspace security cooperation accessible to individuals new to the field.

For experienced policymakers and practitioners, this book goes beyond the basics. We explore advanced strategies, emerging trends, and international best practices in cyber capacity building and international cooperation. Through the insights of renowned contributors, we offer numerous case studies and valuable insights that can inform decision-making processes and enhance the effectiveness of seasoned professionals supporting security cooperation roles within the DOD and beyond.

Throughout the book, we emphasize the real-world applicability of cyberspace security cooperation. We address the geopolitical considerations that shape international collaborations, delve into the legal frameworks governing cyber investment and cooperation activities, and discuss the role of technical innovations and emerging technologies in

bolstering cyber defenses. By grounding our discussions in practicality, we seek to equip readers with the knowledge and tools necessary to navigate the ever-evolving landscape of cyberspace security cooperation.

We acknowledge that cyberspace security cooperation comes with its own set of challenges. Conflicting national interests, divergent legal frameworks, and political influences can complicate efforts to forge effective partnerships. To address these complexities, we present nuanced discussions that encourage critical thinking and foster informed dialogue. By exploring the intersection of national defense strategies and security considerations, we aim to guide policymakers and practitioners in navigating the intricate trade-offs inherent in this field.

To newcomers, we extend our warmest welcome and encourage you to embrace the exciting and ever-evolving field of cyberspace security cooperation. For experienced practitioners and policymakers, we express our gratitude for your dedication and unwavering commitment to defending our digital future.

We hope that “Defending the Future: U.S. Cyberspace Security Cooperation Post the Ukraine War Era” serves as a valuable companion on your journey. May its insights inspire collaboration, foster innovative approaches, and empower individuals and organizations to effectively address the challenges of our interconnected world. Together, let us embark on this vital mission to safeguard our digital landscape for generations to come.