

Global Cyber Defense Agile Strategy

This document outlines the Global Cyber Defense Agile Strategy, designed to provide a flexible and adaptive framework for addressing the complex challenges of modern cyber threats.

The strategy is built on the principles of agility, collaboration, and continuous improvement, emphasizing the need for a dynamic approach to cybersecurity.

The strategy is organized into several key components:

- Strategic Vision:** A clear understanding of the organization's mission and the specific cyber threats it faces.

- Agile Methodology:** The use of iterative development and testing cycles to rapidly identify and respond to threats.

- Collaboration:** A cross-functional team approach involving IT, legal, and business units to ensure a holistic defense strategy.

- Continuous Improvement:** Regular reviews and updates to the strategy based on new threat intelligence and organizational needs.

The strategy will be implemented through a series of phases, each focusing on a specific aspect of the organization's cybersecurity posture:

- Phase 1: Assessment and Planning** (Weeks 1-4)

- Phase 2: Development and Testing** (Weeks 5-8)

- Phase 3: Deployment and Monitoring** (Weeks 9-12)

- Phase 4: Review and Iteration** (Weeks 13-16)

This iterative process will continue throughout the year, allowing the organization to stay ahead of emerging threats and maintain a strong cybersecurity posture.

We are committed to the success of this strategy and believe it will lead to a more secure and resilient organization.

If you have any questions or concerns, please do not hesitate to reach out to us.

Thank you for your attention and support.

Aymen Gatri & Sana Al Qayyum

Global Cyber Defense Agile Strategy

4th Army Dimensional Doctrine

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische
Daten sind im Internet über <http://dnb.ddb.de> abrufbar

Bild auf dem Umschlag:
Designed by Freepik
Futuristic-technology-screen-interface
business-corporate-protection-safety-security-
concept

ISBN 978-3-96138-207-1

© 2020 Wissenschaftlicher Verlag Berlin
Olaf Gaudig & Peter Veit GbR
www.wvberlin.de / www.wvberlin.com
Alle Rechte vorbehalten.
Dieses Werk ist urheberrechtlich geschützt.
Jede Verwertung, auch einzelner Teile, ist ohne
Zustimmung des Verlages unzulässig. Dies gilt
insbesondere für fotomechanische Vervielfältigung
sowie Übernahme und Verarbeitung in EDV-Systemen.

Druck und Bindung: SDL – Digitaler Buchdruck, Berlin
Printed in Germany
€35,00

Contents

I.	Introduction	9
II.	Background.....	12
CHAPTER 1.....		15
1.1.	The Challenge within the Fourth Dimension Battlefield.....	15
1.2.	Directed Energy: The Battle for the EM Spectrum.....	16
1.3.	Agile Coherent Cyber- strategies	17
1.4.	Coherent Agile Approach	19
1.5.	Investment in integration: Enhancing the Integrated ICT capability	21
1.6.	Summary	23
CHAPTER 2.....		24
	Maritime Cyber Security	24
2.1	Maritime Cybersecurity Threads	24
2.2	Classification of Maritime Cyber Threat	25
2.2.1	System Susceptibility	26
2.2.2	Hijacking	26
2.2.3	Out-of-date software	27
2.2.4	Cost and Profit	27
2.2.5	Mitigation	28
2.2.6	Sum-up of Maritime Cyber Security	29
CHAPTER 3.....		31
3.1	Cybercrime types.....	31
3.2	Transport Cyber Security	31
CHAPTER 4.....		33
4.1	Russia	33
4.2	Social Networks in Russia	33
4.3	Internet as threat	34
4.4	Cyber Security strategy	35
4.5	Priorities of Strategy Use for Cyber Security	36
4.6	Cyber Security Activities	36

CHAPTER 5.....	38
5.1 Introduction to the UK and EU Cyber Security approaches.....	38
5.2 Objectives.....	39
5.3 UK Cyber Security Strategy.....	39
Moreover, the NCSC CEO Ciaran Martin Said:.....	40
5.4 Advanced availability of internet connectivity	40
CHAPTER 6.....	42
6.1 National Digital Security Strategy.....	42
6.2 Context-People Elope, Economy & State.....	43
6.2.1 Citizens	43
6.2.2 Economy	44
6.2.3 Risks/ Threads.....	45
6.2.4 Government	46
6.3 Critical National Infrastructure	46
6.4 European And International Developments.....	48
6.5 Principles and Guidelines	50
6.5.1 Subsidiarity	50
6.5.2 Risk-Based Methodology and Proportionality	50
6.5.3 Objectives	50
6.6 Measures	51
6.6.1 Build up the Nationwide Digital Security Centre.....	51
6.6.2 System and Data Security for Open Bodies	52
6.6.3 Completely actualize the NISD by methods for essential legislation.....	52
6.6.4 Coherent Universal Commitment	53
6.6.5 Policing and National Security	53
6.7 Cybercrimes	53
6.7.1 Common Military Collaboration	54
6.7.2 Basic Framework	55
6.7.3 Data Sharing	56
6.7.4 Instruction and preparing for Industry/SMEs	57
6.7.5 Open Mindfulness	57

6.8	Coherent EU Cyber Security.....	57
6.8.1	Coherence Strategies Challenges.....	59
6.9	Why build a Coherent Cyber Security Strategy?	62
6.9.1	Shrewd Cyber Actors	63
6.9.2	Reasonable Cybersecurity Strategies	64
6.10	Technology is disrupting the financial services industry	65
6.11	Sum-up.....	66
	CHAPTER 7.....	68
7.1	Cybercrime Terrifying and Cyber Security Statistics and Trends	68
7.1.1	Strategies to Stay Safe.....	68
7.1.2	Cybercrime Statistics and Proofs	68
7.2	The big Picture of Cybercrime Statistics	70
7.3	Effects of Cybercrimes on Consumers	72
7.4	The Cumulative Cost of Scammer/ Cybercrimes.....	75
7.5	Industries/Business progressively receiving end of hacks and cracks	77
7.6	Statics of Cyberbullying	78
7.7	Cybercrime and Cyber Security Predication for 2018-2019	80
7.8	Cybercrime and Cybersecurity Surrey's, Studies, Trends and the Reports	81
7.9	Seven Ways to Improve the Online Privacy and Security Quick Wins	88
7.10	The Fifth Commandment in the Artificial Intelligence AI War	92
7.10.2	Weapons with Judgment.....	92
7.10.3	FCAS, the Air Defense of the Future	93
7.11	Summary	94