

Dominance on The Digital Battlefield

Or: Why Cyber Weapons are
Cooler than Nukes (pun intended)

Lars Hilse



IPS Press is the publishing arm of the Institute of Policy Studies, Islamabad – an independent think tank dedicated to promoting policy-oriented research, dialogue, and human & technological development for better governance. Pakistan Affairs, International Relations, Faith and Society, Governance and Leadership, and Science and Technology are some of the major study areas at IPS.

Dominance on The Digital Battlefield

Or: Why Cyber Weapons are Cooler than Nukes (pun intended)

Author: Lars Hilse

ISBN: 978-969-448-847-9

Edition: 1st

© IPS Press 2025

All rights reserved. No part of this publication may be reproduced, translated, stored in a retrieval system, or transmitted in any form or by any means without prior written permission from the Institute of Policy Studies, Islamabad.

Inquiries concerning reproduction should be sent to IPS Press at the contact details given below:

IPS Press

Institute of Policy Studies

Nasr Chambers, 1, MPCHS Commercial Centre, E-11/3,
Islamabad, Pakistan

Tel: +92 51 8438391-3, 8438388

Email: publications@ips.net.pk | URL: www.ips.org.pk

Title Design: Lars Hilse

Layout: Abid Hussain

CONTENTS

Acknowledgements

Foreword

Preface

Author's 60 Second Bio

Introduction

Pars Pro Toto

So, Why Are Cyber Weapons Cooler than Nukes?

The Military Context?

1. Welcome to the Digital Battlefield

1.1. Cyber Domain has become Critical New Frontline

1.2. Cyber Weapons Level the Playing Field Against Advanced Militaries

1.3. Custom Tools Developed for Espionage, Disruption, and Destruction

2. Cyber Weapon Capabilities

2.1. Infiltration Tools Enabling Access to Sensitive Networks .

2.2. Malware Designed to Exfiltrate Classified Data Undetected

2.3. Viruses tailored to sabotage Infrastructure and Weapons Systems

2.4. Information Warfare Usage

2.5. Artificial Intelligence (AI), and Artificial General Intelligence on the Modern Battlefield

3. Attribution Challenges

3.1. Apparent Nation-State Origins, but Difficulty Proving Attribution

3.2. Use of Third Parties or Hacking Groups for Plausible Deniability

4. Unique Properties of Cyber Weapons

4.1. Offensive Cyber Weapons Outpace Defensive Capabilities

5. Recommendations

5.1. Robust, and Hardened Cybersecurity Infrastructure

5.2. Specialised Cyber Defence Units

5.3. Domestic Surveillance Legislation

5.4.	Active Cyber Defence	
5.5.	Offensive Capabilities	
5.5.1	Acquiring Cyber Weapons.....	
5.6.	Counter-Propaganda	
5.6.1.	The Educated Public	
5.6.2.	Establishing the Counter-Propaganda Centre	
5.7.	International Cyber Treaties	
5.8.	Protecting Key Infrastructure.....	
5.8.1.	The Importance of Protecting Key Infrastructure from Cyberattacks	
5.8.2.	Key Infrastructure Sectors	
5.8.3.	Protecting Key Infrastructure: A Realistic Approach	
5.9.	Improving National Cyber Hygiene.....	
5.9.1.	Cybersecurity Education Can't Start Early Enough	
5.9.2.	Cybersecurity Education for the General Population	
5.9.3.	Technology Innovation, Securitisation, and Deployment	
5.9.4	Policy, and Regulation Enhancement/Modernisation	
5.9.5.	Constant Exploration of Futuristic Solutions	
5.9.6.	Cyber Hygiene and the Military	
5.10.	Diversifying Technology Supply Chains	
5.10.1.	Reasons for Creating Diversified Technology Supply Chains	
5.10.2.	Strategising a Diversified Supply Chain	
5.11	Cyber Weapons in Defence Exports	
6.	Conclusion: Securing the Future of National Defence	
7.	Glossary of Terms	
8.	Index	

