Victor Vevera

SECURITATE ŞI PUTERE ÎN SPAȚIUL CIBERNETIC



editura militară

53.

II 41.824 Q1

VICTOR VEVERA



SECURITATE ȘI PUTERE ÎN SPAȚIUL CIBERNETIC





EDITURA MILITARĂ
BUCUREȘTI, 2017

CUPRINS

1. ASPECTE TEORETICE 9
1.2. Dezintegrarea digitală 14
1.3. Atacul vs apărarea în spațiul cibernetic 15
1.4. Interconectivitatea, complexitatea și riscurile sistemice 17
1.5. Rolul organizațiilor naționale de securitate 18
1.6. Cel mai grav scenariu: „Cybergeddon": – Armaghedonul cibernetic 21
1.7. O chestiune de încredere 22

2. VULNERABILITĂȚI ȘI AMENINȚĂRI ÎN SPAȚIUL CIBERNETIC 25
2.1. Vulnerabilități/factori de risc la adresa elementelor informatice și informaționale 25
2.2. Amenințări și vulnerabilități: o problemă cu cinci niveluri 26

3. SECURITATE CIBERNETICĂ ȘI OPORTUNITĂȚI DE COST 31
3.1. Elemente de management al riscului 31
3.2. Asigurarea securității cibernetice 31

4. ASPECTE PRACTICE: STUDIU DE CAZ PE DIFERITE ȚĂRI 33
4.1. Brazilia 36
4.2. China 37
4.3. Estonia 38
4.4. Federația Rusă 42
4.5. Regatul Unit al Marii Britanii 43
4.6. Statele Unite ale Americii 44
4.7. Proiect UE 2001-2004 47
4.8. România 47

5. INFRASTRUCTURI CRITICE CIBERNETICE 53
5.1. Definirea conceptului de infrastructură 53
5.2. Infrastructura informațională națională (IIN) 56
5.3 Definirea conceptului de infrastructura critică 57
5.4. Definirea conceptului de infrastructura critică cibernetică 62
5.5. Provocări globale, pericole, amenințări și agresiuni posibile la adresa infrastructurilor critice. Vulnerabilități specifice 63
5.6. România, cele mai pregnante vulnerabilități 67
5.7. Factorii de risc la adresa infrastructurilor critice 68
5.8. Amenințările la adresa infrastructurilor critice 68

6. TIPOLOGIA PERICOLELOR ȘI AMENINȚĂRILOR LA ADRESA INFRASTRUCTURILOR CRITICE 71
6.1. Stările de pericol 71
6.2. Stuxnet, prototipul unei arme cibernetice 75
6.3. Web-ul negru: ce este, cum lucrează și de ce nu va dispărea 80

7. PROTECȚIA INFRASTRUCTURILOR CRITICE CIBERNETICE ... 84

8. PROTECȚIA INFRASTRUCTURILOR INFORMAȚIONALE CRITICE (CIIP) 96
8.1. Rolul CIIP 96
8.2. Prevenția și alertarea timpurie 97
8.3. Detecție 99
8.4. Reacția 100
8.5. Managementul crizelor 101
8.6. Concluzii 106

9. NORMATIVE EUROPENE ȘI NAȚIONALE ÎN DOMENIUL DE REFERINȚĂ 110

10. PLANUL UE ÎN DOMENIUL SECURITĂȚII CIBERNETICE PENTRU PROTEJAREA INTERNETULUI DESCHIS, A LIBERTĂȚII ONLINE ȘI A OPORTUNITĂȚILOR GENERATE DE INTERNET 118
10.1. Programul european privind protecția infrastructurilor critice 118
10.2. Partajarea informațiilor referitoare la Protecția infrastructurilor critice (PIC) 120

10.3. Protecția infrastructurilor critice naționale (ICN) 121
10.4. Contextul istoric 122
10.5. Propunere de decizie a Consiliului privind rețeaua de alertă privind infrastructurile critice (CIWIN) {SEC(2008)2701} {SEC(2008)2702} /*COM/2008/0676 final – CNS 2008/0200*/ 124

11. ABORDAREA PROTECȚIEI INFRASTRUCTURILOR CRITICE ÎN DIFERITE STATE ALE LUMII 152

12. PROTECȚIA INFRASTRUCTURILOR CRITICE ÎN ACTELE NORMATIVE NAȚIONALE 155

13. ORGANISME LA NIVEL NAȚIONAL CU ATRIBUȚII ÎN DOMENIUL SECURITĂȚII CIBERNETICE 156
13.1. Consiliul Operativ de Securitate Cibernetică (COSC) 156
13.2. Centrul Național de Securitate Cibernetică (CNSC) 157
13.3. Sistemului Național de Alertă Cibernetică (SNAC) 157

14. DEFINIREA CERT-RO – HOTĂRÂREA NR. 494/2011 PRIVIND ÎNFIINȚAREA CENTRULUI NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ –CERT-RO 159

15. STRATEGIA NAȚIONALĂ PRIVIND PROTECȚIA INFRASTRUCTURILOR CRITICE 1473/2011 160

16. ALTE HOTĂRÂRI 162

17. H.G. NR. 271/2013 PENTRU APROBAREA STRATEGIEI DE SECURITATE CIBERNETICĂ A ROMÂNIEI ȘI A PLANULUI DE ACȚIUNE LA NIVEL NAȚIONAL PRIVIND IMPLEMENTAREA SISTEMULUI NAȚIONAL DE SECURITATE CIBERNETICĂ 163

18. LEGEA PRIVIND SECURITATEA CIBERNETICĂ A ROMÂNIEI 168

19. ANEXĂ – ACTE NORMATIVE CONEXE DOMENIULUI PROTECȚIEI INFRASTRUCTURII CRITICE 172

20. REGLEMENTĂRI SPECIFICE PRIVIND PROTECȚIA FIZICĂ DOMENIUL NUCLEAR 174

TERMENI ȘI DEFINIȚII 175

LISTA DE ABREVIERI 179

BIBLIOGRAFIE 183