

OBSAH

Úvod	7
1. Súhrnný prehľad prístupov v boji proti využitiu kyberpriestoru násilnými extrémistami.....	11
1.1. Úvod do súhrnného prehľadu prístupov v boji proti využitiu kyberpriestoru násilnými extrémistami	11
1.2. Úrad pre kybernetickú bezpečnosť a informačné zabezpečenie (OCSIA) v Spojenom kráľovstve	12
1.3. Využitie internetu pre teroristické účely (dokument UNODC).....	15
2. Postupy proti propagande násilných extrémistov v kyberpriestore	19
2.1. Úvod do problematiky propagandy násilných extrémistov v kyberpriestore.....	19
2.2. Rakúsky zákon o symboloch.....	21
2.3. Postih propagácie internetovej prezentácie Národného odporu v ČR.....	23
3. Postupy proti online radikalizácii násilných extrémistov	27
3.1. Úvod do problematiky online-radikalizácie násilných extrémistov	27
3.2. Boj proti online-radikalizácii – akčná stratégia ICSR.....	29
3.3. Indikátory islamskej radikalizácie podľa Brandenburského úradu na ochranu Ústavy.....	32
4. Postupy proti nenávisťným prejavom v kyberpriestore a kyberšikane s extrémistickým podtextom.....	35
4.1. Úvod do postupov proti nenávisťným prejavom v kyberpriestore a kyberšikane s extrémistickým podtextom	35
4.2. Pozičný dokument írskej právnej komisie o „Kyberkriminalite týkajúcej sa osobnej slobody, súkromia a povesti vrátane kyber-šikany“	38
4.3. Prípád Alpen-donau.info.....	40
5. Postupy proti využitiu kyberpriestoru ako výcvikového, plánovacieho, logistického a finančného priestoru násilných extrémistov	43

5.1.	Úvod do postupov proti využitiu kyberpriestoru ako výcvikového, plánovacieho, logistického a finančného priestoru násilných extrémistov	43
5.2.	Využitie ICQ komunikácie ako dôkazu pri dokazovaní prípravy extrémistického násilia v ČR.....	45
5.3.	Monitoring nebezpečných prejavov online – UMATI	48
6.	Postupy proti kyberterorizmu, kybernetickej špionáži a kybernetickým vojnovým útokom s extrémistickým podtextom.....	51
6.1.	Úvod do postupov proti kyberterorizmu, kybernetickej špionáži a kybernetickým vojnovým útokom s extrémistickým podtextom.....	51
6.2.	Estónska Stratégia kybernetickej bezpečnosti na roky 2014–2017.....	53
6.3.	Zákon o kybernetickej bezpečnosti v Českej republike	55
7.	Dokazovanie extrémistickej trestnej činnosti v kyberpriestore	59
7.1.	Úvod do dokazovania trestnej činnosti v kyberpriestore.....	59
7.2.	Dokument „Sprievodca forezným IT“ od Spolkového úradu pre bezpečnosť v informačnej technike	61
7.3.	Dokazovanie vo veci internetovej stránky Bohemia Hammer Skins.....	62
8.	Všeobecná osvetová činnosť proti zneužitiu kyberpriestoru násilnými extrémistami.....	67
8.1.	Úvod do všeobecnej osvetovej činnosti proti zneužitiu kyberpriestoru násilnými extrémistami	67
8.2.	Jugendschutz.net	68
8.3.	Vzdelávacie a osvetové aktivity Väzenskej služby ČR proti extrémistickým prejavom vo väzení so zameraním na kyberpriestor	70
	Záver	73
	Summary	75
	Zoznam zdrojov a literatúry	77
	Zoznam skratiek.....	83
	Menný a vecný register	84