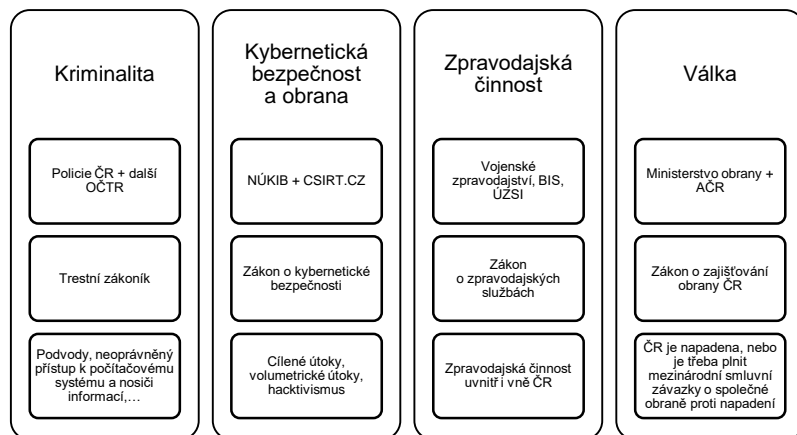


## 1 Model 4 sil

Dosavadní praxe ukázala, že stávající zákony stačí k pokrytí všech oblastí, jež řeší novela ZoVZ. Činnosti shrnuje model:



## 2 Eskalační model s předáváním metadat (NetFlow) a společné operační centrum

Při NÚKIB bude zřízeno společné centrum kyb. obrany s participací operátorů, všech zprav. služeb a Policie. Centrum organizuje obranu KII v ČR. Inspirace zákonem ZKB, § 21 a jeho rozšíření o stav „kybernetického konfliktu“. Viz tabulka:

Eskalační stupeň	Činnost NBÚ	Činnost VZ	Činnost ISP
0 (bdělost)			Běžná činnost
1 (stav kybernet. nebezpečí)	Vyhlašuje „stav kybernetického nebezpečí dle ZKB“	Pasivně monitoruje provoz	Umožní VZ pasivní monitoring provozu
2 (stav kybernet. konfliktu)		Aktivuje a využívá prvky KO	Umožní činnost VZ dle eskalačního stupně 1 a současně využití prvků KO

## 3 Model sdílené kybernetické obrany

Zákon el. komunikací ukládá povinnost umožnit odposlech nejen datové komunikace vybraným zpravodajským službám a Policii.

Provoz prvků kybernetické obrany může být ve stejném režimu. Prvky by byly vlastněny a spravovány operátorem, přičemž by byly stávající zákony upraveny tak, aby „cílenou detekci jevů nasvědčujících o existenci kybernetického útoku“ mohli na vyžádání – podobně jako nyní – provádět všechny subjekty (PČR, NÚKIB, VZ, BIS a ÚZSI). Byl by standardizován formát, ve kterém by byly „signatury“ jevů operátorům distribuovány a detekované „jevy“ zasílány žadateli.

Tento model využívá stávajících ochranných mechanismů tak, aby „nástroje detekce“ a kybernetická obrana obecně nebyly zneužity a současně umožní participaci všem subjektům tak, aby mohla být obrana KII efektivní.

## 4 Pět požadavků ICTU

ICTU dlouhodobě požaduje zákonnou garanci alespoň následujících požadavků:

### Zajištění důvěrnosti komunikací

„nástroje detekce“ nesmí umožnit sběr obsahu přenášených dat ani jakkoli narušovat jejich kryptografickou ochranu

### Garance pasivních prvků

pasivita „nástrojů detekce“ garantuje jak předchozí bod, tak chrání infrastrukturu

**Zbavení odpovědnosti za škodu třetím stranám** (případně provozovateli v souvislosti s provozem zařízení)  
činnost VZ v infrastruktuře operátora může být příčinou výpadků nebo zhoršení kvality poskytované služby zákazníkům

### Stanovení povinnosti uzavřít smlouvu

smlouva jednoznačně definuje umístění „nástrojů detekce“, garanci dostupnosti, přístupu k zařízení a datům, technická omezení atd.

### Provoz a zřízení budou na náklady žadatele

veškeré náklady na provoz a pořízení zařízení, včetně energií a místa v datovém rozvaděči budou na náklady VZ