Současné formy kybernetické kriminality a možnosti jejich postihu

Prof. Ing. Vladimír Smejkal, CSc. LL.M.
Vysoké učení technické v Brně
rektor Moravské vysoké školy Olomouc

Kybernetická kriminalita

Definice kyberprostoru

Termín kyberprostor (angl. cyberspace) použil údajně jako první americký spisovatel William Gibson na počátku 80. let ve své povídce Jak vypálit Chrome. (+ Neuromancer)

Umělecká vize nemá nic společného se současným chápáním kyberprostoru jako něčeho, co spíše intuitivně, nežli striktně vědecky chápeme jako nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů.

Podle § 2 písm. a) ZKB *se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*

Víme, co to je „Kybernetická kriminalita“?

Kybernetická kriminalita

Kybernetická kriminalita je nástupcem kriminality počítačové, charakterizované jako páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď

a) jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité,

b) nebo jako nástroj trestné činnosti.

Definice kyberprostoru

Dnes se útoky odehrávají v kyberprostoru tvořeném počítačovými sítěmi a jednotlivými prvky těchto sítí, mající přidělenu svoji IP adresu. Tedy cokoliv, co umí prostřednictvím protokolu TCP/IP či nějakého jiného komunikovat s jinými prvky v kyberprostoru. (Viz IoT.)

Lze tedy konstatovat, že

kybernetická kriminalita je trestná činnost odehrávající se v kyberprostoru.

„Stará“ kybernetická kriminalita

- **podvody,**
- **porušování autorských práv** (nepříliš vhodně, leč populárně označované jako počítačové pirátství),
- **útoky na funkčnost počítačových systémů** (pomocí virů),
- **neoprávněné nakládání s osobními údaji,**
- **neoprávněné užívání počítačů a dalších zařízení** (od počítačů k WiFi),
- různé druhy skutkových podstat spojených s **šířením informací** (*pornografie, nebezpečné vyhrožování a pronásledování*, *nekalá soutěž)*

Změna kvality kyberkriminality

Přelom 20. a 21. století je současně i přelomem mezi „starými“ a „novými“ formami kybernetické kriminality.

Od „soukromých“ hackerů a útokům na peníze jsme se posunuli k ptokům „státním“ a útokům na kritickou infrastrukturu a/nebo ideologickým a propagačním.

Útoky mají asymetrický charakter, ve formě tzv. kybernetické války mohou s relativně nízkými náklady paralyzovat veškerá spojení, dopravu, energetické systémy, bankovnictví, průmysl i obranné prostředky technologicky vyspělejší země.

Dnes to jsou a očekáváme, že ještě více budou:

1. *KYBERTERORISMUS* v podobě útoků na funkčnost počítačových systémů a elektronických komunikací (DoS / DDoS, malware a spyware, elektromagnetické útoky atd.), tj. trestné činy jako *obecné ohrožení, poškození a ohrožení provozu obecně prospěšného zařízení, sabotáž,*
2. *ÚTOKY NA OBSAH počítačových systémů a předávaných zpráv* (*vyzvědačství, ohrožení utajované informace*),
3. *ŠÍŘENÍ INFORMACÍ* ve prospěch útočníka a/nebo v neprospěch protivníka, případně ovlivňující třetí strany.

Skutkové podstaty spojené se **šířením informací**

- *Násilí proti skupině obyvatelů a proti jednotlivci,*
- *Hanobení národa, rasy, etnické nebo jiné skupiny osob,*
- *Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod,*
- *Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka,*
- *Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka,*
- *Popírání, zpochybňování, schvalování a ospravedlňování genocidia,*
- *Podněcování k trestnému činu*
- *Schvalování trestného činu.*

„Kybernetické“ trestné činy

Aby mohly být realizovány uvedené kriminální aktivity, dochází obvykle k naplnění skutkovbých podstat trestných činů:

- § 230 **Neoprávněný přístup k počítačovému systému a nosiči informací**
- § 231 **Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.**

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části,…

…není třeba žádné další jednání pachatele,

…musí ale překonat bezpečnostní opatření.

Postih jednání „jen to zkusím“, „ jen se podívám“ (změna oproti předchozí právní úpravě.)

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací /dále jen PS-NI/ a

a) neoprávněně užije data uložená v PS-NI,

b) data uložená v PS-NI neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v PS-NI tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do PS-NI nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

bude potrestán…

Kdo jsou pachatelé kybernetické kriminality?

Útočníci


CIZÍ STÁTY


TERORISTÉ


ZAMĚSTNANCI


ORGANIZED CRIME
Money • Power • Respect
ORGANIZOVANÝ ZLOČIN

Boj proti kybernetické kriminalitě

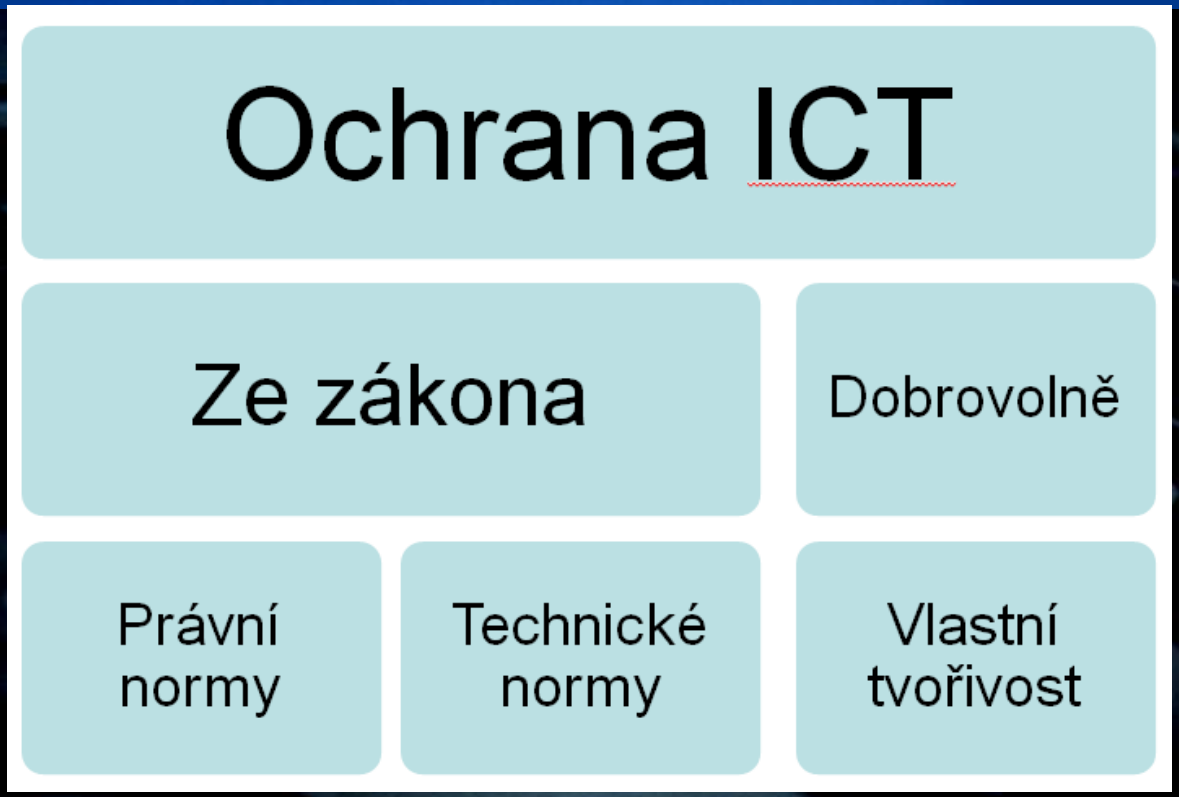
PREVENCE

1. **budování zabezpečených ICT,**
2. výchova k bezpečnosti,
3. výzkum základní i aplikovaný,
4. mezinárodní spolupráce.

REPRESE

1. problém jurisdikce,
2. problém odhalování trestné činnosti,
3. problém dokazování,
4. problém některých skutkových podstat nového trestního zákoníku, resp. chybějících skutkových podstat.

Přístupy k budování zabezpečených ICT systémů



Budování zabezpečených ICT systémů je nutnou podmínkou pro „přežití“ kybernetického útoku.

PREVENCE na prvním místě!

Jak dosáhnout větší efektivity trestního stíhání pachatelů kybernetické kriminality?

- Používáním nástrojů, které jsou schopny zavčas odhalit, že došlo k mimořádné události (logy + analýza).
- Zadokumentovat, co se v systému stalo a co nejrychleji takové podezření oznámit kvalifikovaným orgánům činným v trestním řízení.
- Zachování IS v takovém stavu, aby nebyly stopy smazány, a zachování důvěrnosti tak, aby pachatel, který se ve většině případů nachází na důvěryhodném místě v řadách zaměstnanců organizace, nebyl varován.
- Fyzické a datové objekty se stávají důkazy teprve tehdy, jsou-li akceptovatelné příslušnými orgány. Klíčová je prokazatelnost, že se stopa nacházela na určitém místě a že od jejího zajištění do ukončení znaleckého zkoumání nebyla žádným způsobem modifikována.

Co nás čeká?

KYBERVÁLKY A KYBER TERORISMUS

- Internet věcí – aneb každý přístoj ve firmě i doma připojený k Internetu,
- BYOD – přineste si vaše vlastní zařízení do firmy,
- Útoky prostřednictvím sociálních sítí – se od informačních útoků (nakládání a šíření informací) přesouvají stale vice k podvodům a šíření škodlivého software
- Útoky na technologické řídicí systémy - od obecného ohrožení po ublížení na zdraví.
- **Útoky na informační a komunikační infrastrukturu státu.**

Závěr

- Čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití musíme počítat. *Nebudou to aktivity soukromníků, ale států…*
- Jsou právní řády, včetně oborů práva trestního, kriminologie a kriminalistiky budou dostatečně připraveny na technologický i společenský vývoj?
- Prevence je důležitější než represe.
- Úspěšný postih pachatelů KK zahrnuje právní procesní a hmotnou složku, existenci skutkových podstat a zvládnutí dokazování.

Literatura:
vše o kybernetické kriminalitě

SMEJKAL, Vladimír.

***Kybernetická kriminalita*.**

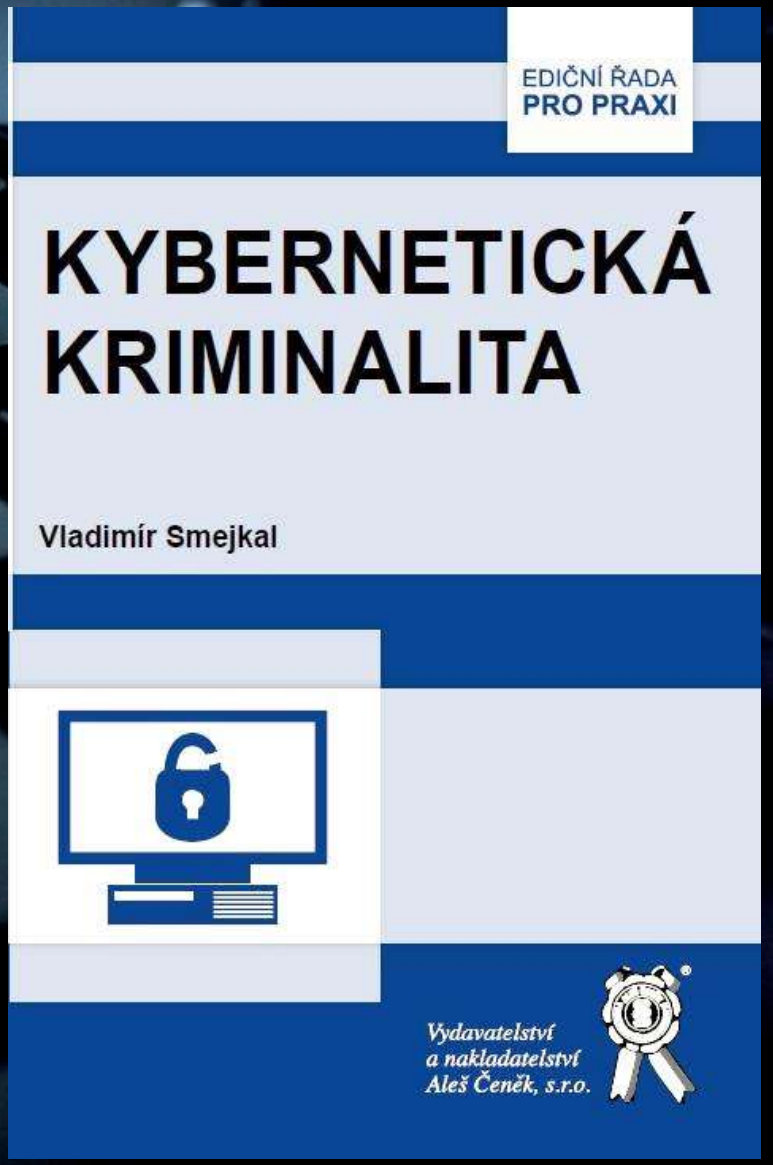
Plzeň:

Nakladatelství Aleš Čeněk,

2015.

636 stran.

ISBN 978-80-7380-501-2.



Literatura:
vše o kriminalistice

Porada Viktor a kolektiv.

KRIMINALISTIKA

Technické, forenzní a kybernetické aspekty.

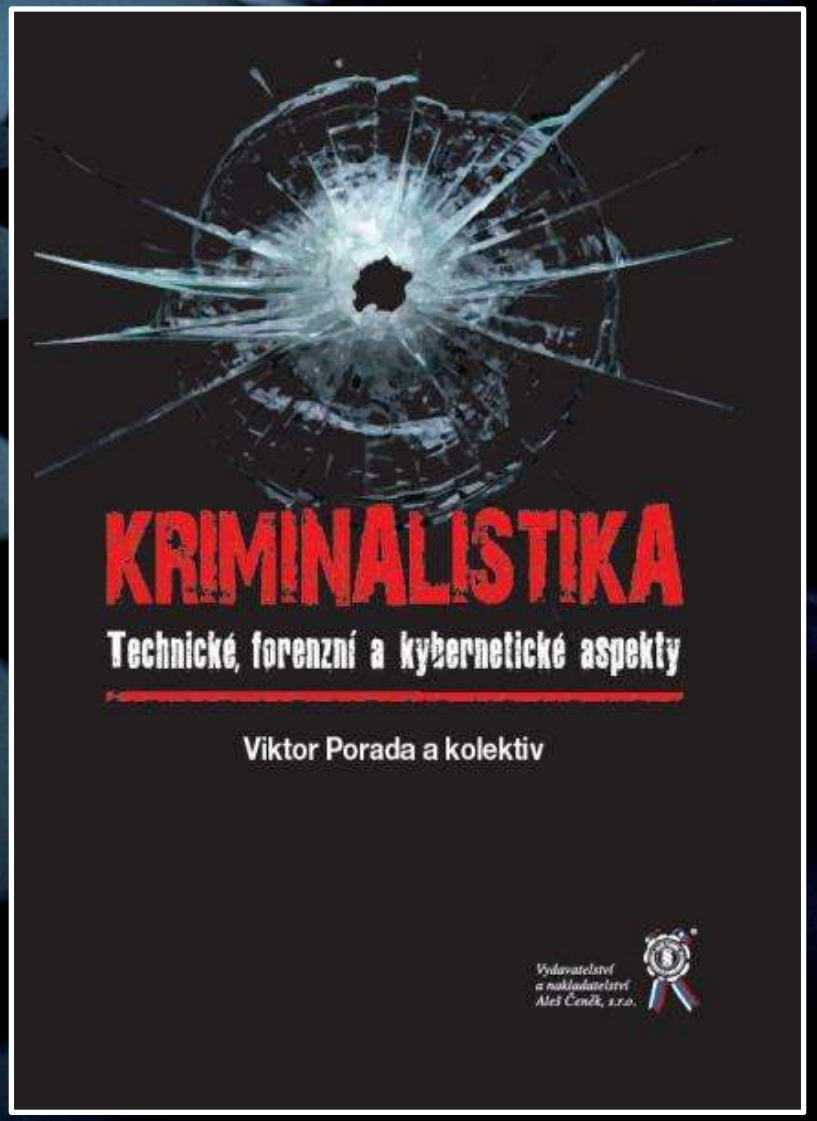
Plzeň:

Nakladatelství
Aleš Čeněk,

2016.

1024 stran.

ISBN 978-80-7380-589-0.



Děkuji za pozornost.

Kontakt:

smejkal@znalci.cz