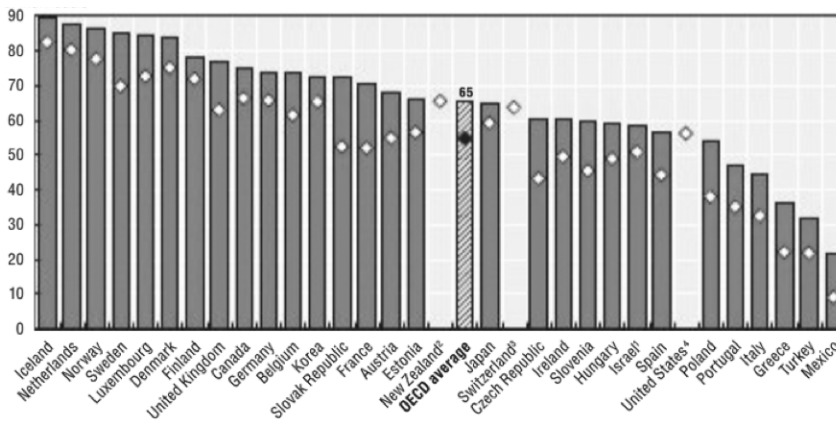
KAPITOLA 1

Pojem kyberkriminalita a příbuzné pojmy

1.1 Kyberkriminalita

Podle údajů Eurobarometru (Evropská komise – EK, 2011) používá 44 procent Evropanů internet každý den (EU27)[1]. Slovinsko je počtem uživatelů, kteří internet používají každý den, s 47 procenty blízko průměru, je to sice téměř dvakrát více než v Řecku, Portugalsku a Rumunsku (země na posledních třech místech), ale stále ještě téměř o polovinu méně než v Nizozemsku, Dánsku a Švédsku (země na prvních třech příčkách; EK, 2011) (viz údaje o členských zemích OECD na obrázku 1).

Obrázek 1: Jednotlivci používající internet v letech 2010 a 2007[2]



Na konci roku 2010 bylo ve Slovinsku 1 486 360 majitelů mobilních telefonů s uživatelskou smlouvou a 635 590 majitelů mobilních telefonů s předplacenými

[1] V tomto příspěvku hovoříme o internetu v širším smyslu, zahrnuje např. e-maily, webové stránky, blogy, chaty, fóra, sociální sítě (například Facebook, Twitter, Google+), stránky určené ke sdílení multimediálních příspěvků (například Picasa, YouTube).

[2] OECD, 2012a.

kartami (Zupan, 2011), což představuje přibližně jeden mobilní telefon na obyvatele. Penetrace používání internetu a mobilních telefonů je tedy velmi vysoká a lze usuzovat, že se ve Slovinsku bude procentuálně nadále zvyšovat a bude se přibližovat rozvinutějším zemím.

Široký rozmach informačních technologií znamená velkou výhodu pro jednotlivce, hospodářské subjekty a společnost jako celek, ale přináší i nová rizika, například nebezpečí úniku obchodních a osobních údajů. Na začátku osmdesátých let se zdálo, že hlavním přínosem rozvoje elektroniky a mikroprocesorů a jeho základní platformou bude osobní počítač. Zneužití s ním spojená byla nazvána počítačovou kriminalitou (něm. *Computerkriminalität*). Jelikož je pojmenování kriminality podle použitého prostředku nezvyklé, navrhla trestněprávní teorie (Jakulin, 1996) používání označení kriminalita spojená s počítači (angl. *computer-related crime*) (Brvar, 1982), které mělo obsáhnout trestné činy, v nichž počítač figuruje jako nástroj nebo jako předmět útoku. Jelikož je však pro vykonání takového trestného činu zapotřebí určitých znalostí z oblasti výpočetní techniky či informatiky, navrhli autoři také slovní spojení kriminalita v informatice (fr. *la criminalité informatique*).

Pozdější rozvoj vedl k novým terminálovým zařízením (např. mobilní telefony, palmpady, tablety, automatizovaná rozhraní), jejichž společným jmenovatelem se stala data[3] a (komunikační) síť. Tu tvoří terminálová zařízení, servery a směrovače, proto se používal i pojem kriminalita informačně-komunikační technologie (IKT). Ale také elektronických komunikačních sítí je dnes několik druhů. Kromě pevných a mobilních sítí existuje ještě jeden speciální typ sítě – internet, který ke komunikaci využívá speciální protokol (IP – *internet protocol*). V rámci internetu existuje několik způsobů komunikace, respektive poskytování služeb: (1) světový web (www – *world wide web*) pro webové stránky, (2) elektronická pošta, (3) internetový chat v reálném čase (např. *internet relay chat* – IRC), (4) přenos souborů (FTP – *file transfer protocol*), (5) internetové telefonování (VoIP – *voice over internet protocol*) atd. Odsud vyplývá pojetí, že se při využívání těchto služeb a páchání trestných činů na internetu jedná o internetovou kriminalitu (něm. *Kriminalität im Internet*), e-kriminalitu, virtuální kriminalitu nebo kriminalitu na počítačových sítích (angl. *computer network crime*).[4]

[3] Rozdíl mezi daty (angl. *data*) a informacemi (angl. *information*) je v tom, že data jsou „sdělení v podobě, kterou lze zpracovávat počítačově“, zatímco informace představují data zpracovaná a zobrazená tak, že jsou srozumitelná pro uživatele. Informace může obsahovat více dat a podstata dat spočívá v možnosti jejich počítačového zpracování (Slovník informatiky).

[4] Růst internetu ve srovnání s dosavadními technologiemi: internet (*www – world wide web*) potřeboval tři roky na to, aby dosáhl svých prvních 50 milionů uživatelů, televize 15 let a rádio 37 let (Naughton, 2003).

Pod vlivem Úmluvy Rady Evropy o kyberkriminalitě z roku 2001 (dále jako: budapešťská úmluva)[5], která je prvním mezinárodním právním aktem v této oblasti, se uplatnil pojem kyberkriminalita, resp. kybernetická kriminalita (angl. *cybercrime*, fr. *la cybercriminalité, le cybercrime*, něm. *Cyber-crime*). Pojem vychází z krásné literatury[6] a pro potřeby trestního řízení[7] je nepříliš vypovídající. Proto se vedle něj používá ještě pojem kriminalita *high-tech* (nebo vysoce rozvinuté technologie, angl. *high-tech crime*), který dává prostor pro zapojování nových technologií, ačkoliv technologická sofistikovanost je doménou například i biotechnologií nebo jaderné technologie.

Jednotná definice kyberkriminality neexistuje v teorii ani legislativě. Zákonodárci zpravidla používají několik pojmů, které zaměňují[8] nebo mezi ně neprávem kladou rovnítko[9]. Vlivná budapešťská úmluva rozlišuje:

1) trestné činy proti důvěrnosti údajů, ucelenosti a dostupnosti počítačových údajů a systémů (kyberkriminalita v užším slova smyslu, respektive „pravá“ kyberkriminalita): protiprávní přístup, protiprávní blokování, poruchy dat, poruchy systémů, zneužití zařízení;

---

[5] Úmluva o kyberkriminalitě (angl. *Convention on Cybercrime*) vstoupila v platnost 1. července 2004, ve Slovinsku platí od 1. ledna 2005. Zákon o ratifikaci Úmluvy o kyberkriminalitě a Dodatkového protokolu k Úmluvě o kyberkriminalitě, který upravuje inkriminaci rasistických a xenofobních činů spáchaných v informačních systémech (MKKKDP), Úřední věstník RS – MP, č. 62/04 (17/04), 16/05 (2/05).

[6] Slovní spojení kybernetický prostor (*cyberspace*) použil poprvé William Gibson ve svém vědecko-fantastickém románu *Neuromancer* vydaném roku 1984, tedy dobrých deset let před vznikem světové sítě. Tento a další příbuzné pojmy (například klon, kyborg, simulakrum, simulace, matrice, hyperrealita) patří do antikulturního kyberpunkového kontextu a z literární a filmové produkce později pronikly do společenskokritické reflexe. K označování virtuálního prostoru se používají ještě pojmy jako cipherspace, kryptoanarchismus, informační dálnice, infosféra, next nature, metavesmír, společenský software (socioware), telepřítomnost.

[7] Pojem kybernetika vychází z řeckého *kybernetes* (*Κυβερνήτης*), tj. kormidelník, vůdce, pilot, a má stejný kořen jako pojmy vláda, vedení. Slovník slovinského spisovného jazyka definuje kybernetiku jako vědu, která zkoumá podobnosti mezi činností strojů a živou přírodou (SSKJ). Lexikon výpočetní techniky a informatiky definuje kybernetiku (*cybernetics*) jako vědu, která zkoumá chování a způsob řízení komplikovaných systémů, jako jsou například těla živočichů nebo stroje. Snaží se při tom jednotnou matematickou teorií popsat různé systémy bez ohledu na jejich hmotnou povahu (mechanickou, chemickou, elektronickou…) (Pahor et al., 2002). Kybernetiku najdeme v lékařství (biokybernetika), biologii, matematice, technologii, fyzice, psychologii, sociologii, sémiotice.

[8] Viz například Doporučení Rady EU (OJ C 187, 3. 7. 2001), které bez vysvětlení používá ještě pojem počítačová síťová kriminalita.

[9] Viz například Komunikace komise [KOM (2000) 890 koneč.], která tuto kriminalitu definuje jako „každou kriminalitu, která zahrnuje využití IKT“, a výslovně klade rovnítko mezi počítačovou kriminalitu, kriminalitu spojenou s počítači, high-tech kriminalitu a kybernetickou kriminalitu (Evropská komise, 2001).

2) trestné činy spojené s počítačem: počítačové padělání a počítačové podvody;
3) trestné činy spojené s obsahem: různé formy trestných činů spojených s dětskou pornografií;
4) trestné činy spojené s porušováním autorských práv a práv příbuzných.

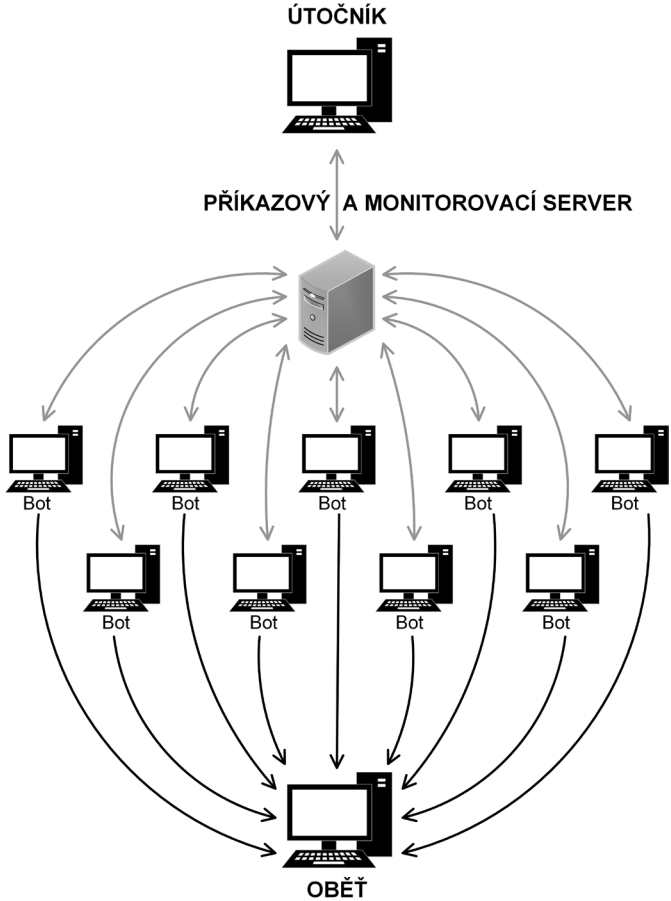
Kyberkriminalitu definují tři hlavní novinky: (1) uskutečňuje se v novém „virtuálním" prostoru; (2) obsahuje nová deviantní chování (podle eliminačního testu je „pravou" kyberkriminalitou taková kriminalita, která by neexistovala bez internetu) a (3) novinky v trestněprávních reakcích (například digitální forenzní analýza).

Dalšími charakteristikami kyberkriminality jsou (Wall, 2007): decentralizovanost (účastní se jí různé delikventní skupiny, které jsou organizovány na síti a jsou specializované), globálnost (dosažitelnost), síťovost, informativnost, distribuovanost (rozptýlenost), automatizovanost (umožnění vzniku individuálních malých, na kumulované úrovni však velkých škod, často méně závislá na „sociálním inženýrství"[10] a formování sítí „odcizených" počítačů, angl. *botnets*[11]).

[10] Sociální inženýrství je oklamání („přelstění") uživatele sloužící k tomu, aby třetí osobě svěřil osobní údaje (například uživatelské jméno a heslo). Pachatel v takovém případě využívá sociálních, nikoliv technických dovedností.

[11] *Botnet* je síť „odcizených" počítačů. *Bot* (zkratka pro roboty) je programový robot, který působí samostatně tak, že pomocí škodlivých programů zasáhne a zneužívá sítě infikovaných a převzatých počítačů (v počítačovém žargonu se jim říká *zombies*). Pro páchání trestných činů pomocí *bots* je charakteristická automatizace, neboť jednou spuštěný program působí samostatně a viktimizačním účinkem takových automatizovaných činů je masovost a poměrně malé škody na zombies. Pachatelé na botnetových sítích používají masové odesílání nevyžádané elektronické pošty, ničení webových stránek, umožňují „podvodné klikání" (angl. *click fraud*), odcizování (angl. *phishing*) sériových čísel aplikací nebo finančních informací k provádění útoků DoS, respektive DDos. Toto ovládání se připisuje zločineckým skupinám z východní Evropy, Běloruska, Ukrajiny, Moldavska a Ruska (Evropské centrum pro boj proti kyberkriminalitě, 2014, s. 26). Jejich rozšíření představuje velkou neznámou. Obecně se má za to, že existuje milion infikovaných „podrobených" počítačů (Reimer, 2007).

Obrázek 2: Síť odcizených počítačů



Legenda:

- tmavá čára – útok na oběť v podobě útoku DDoS (angl. distributed denial-of-service)
- světlá čára – proud příkazů a zpětný proud odcizených informací

Evropské centrum pro boj proti kyberkriminalitě (2014) v EC3 First Year Report identifikuje z hlediska trestněprávních reakcí čtyři nové charakteristiky kyberkriminality, které ztěžují trestní stíhání:

1) přeshraniční povaha internetu umožňuje komukoliv páchání trestných činů proti vládám, právnickým osobám a občanům v Evropě z kteréhokoliv místa na světě. Pronikání do počítačů, krádeže osobních údajů a peněz

na internetu už nejsou logisticky omezeny (například cestováním nebo převážením ilegálního zboží);

2) standardizace softwaru zvyšuje schopnost zvládat stále vyšší počet úkolů a umožňuje pachatelům zvyšovat počet trestných činů na masové úrovni a ovlivňovat miliony počítačů;
3) větší možnost skrývání kriminality používáním technik, jako je přesměrování datového toku, používání anonymizačních nástrojů, používání odcizených identit nebo na dálku odcizených počítačů, používání tajných míst k redistribuci odcizených nebo nelegálních hodnot na „hlubokém" (též neviditelném) internetu (angl. *deep web*), nedohledatelnost kriminálních transakcí z důvodu používání anonymních platebních systémů, jako jsou kryptoměny (například bitcoin), předplacených kreditních karet a dalších anonymních peněžních převodů;
4) spolupráce zločineckých skupin na internetu vedla k většímu rozprostření kriminální činnosti prostřednictvím široce rozvětvených zločineckých sítí.

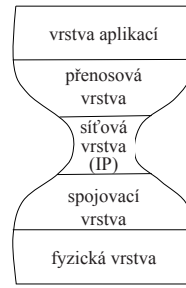
Základními stavebními kameny kyberkriminality jsou informace, počítače a sítě (Walden, 2007). Pojem data (angl. *data*) je širší než pojem informace (angl. *information*): data jsou potenciální informace. Jsou-li přenášena mezi osobou A a osobou B a zůstanou nepochopena, jedná se o data. V opačném případě se z nich stávají informace. Počítač je zpravidla chápán jako celek hardwaru, softwaru a firmwaru (software spojený s hardwarem) a jeho základním úkolem je zpracovávání dat. To znamená, že například USB disk, který do značné míry nahradil různé druhy disket, není počítač a manipulace s ním není součástí počítačové kriminality. Přesto se však definice komplikuje, protože i USB disky a čipové karty (angl. *smart card*) umožňují částečné zpracovávání údajů.

Pachatele kyberkriminality často nazýváme hackery (angl. *hackers*) nebo crackery (angl. *crackers*). Crackeři své znalosti využívají k obohacování nebo bezcílnému vandalismu a v hackerské kultuře nejsou pokládáni za opravdové hackery. Hacker je ten, kdo buduje (například nová spojení), zatímco cracker ten, kdo bourá. Hacker se řídí etikou sdílení a pomoci, cracker etikou apropriace a starosti o sebe sama. Při porušování práv duševního vlastnictví často rozlišujeme mezi černými uživateli a piráty. Prvně jmenovaní porušují práva duševního vlastnictví s cílem získat produkt pro vlastní užití, druzí jsou vedeni motivem zisku z dalších redistribucí pirátských kopií. Vzhledem k lepším technickým znalostem a formálnímu vzdělání hackerů řadíme hackery mezi pachatele kriminality bílých límečků.

1.2 Kybernetická bezpečnost

Kybernetická bezpečnost (angl. *cyber security*) se týká zabezpečení sítí a informací (VOI)[12] před riziky a incidenty, které nejsou nutně spjaté s kriminalitou. „Rizika" jsou v tomto smyslu okolnosti nebo události, které mohou mít negativní účinek na bezpečnost.[13] „Incidenty" jsou okolnosti nebo události, které mají faktický negativní účinek na bezpečnost.[14] Takto široká definice vyplývá ze samotné struktury internetu. Ten představuje síťový technologický systém složený z několika vrstev: na vrcholku internetu figuruje vrstva aplikací (například e-mail), poté následuje přenosová vrstva (například HTTP,[15] SMTP,[16] poté TCP[17] a UDP[18]), internetový protokol (IP), dále spojovací vrstva umožňující komunikaci mezi směrovači různých výrobců (například PPP[19]) a nakonec vrstva (fyzické) infrastruktury (například optické kabely) (viz obrázek 3).

Obrázek 3: Architektura internetu



[12] Viz Společná zpráva pro Evropský parlament, Radu, Evropský hospodářský a sociální výbor a Výbor regionů ze 7. 2. 2013. [JOIN(2013)1 koneč.].

[13] Definice podle článku 3 odst. 3 Návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, Brusel, 7. 2. 2013 COM (2013) 48 koneč.

[14] Definice podle článku 3 odst. 4 Návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, Brusel, 7. 2. 2013 COM (2013) 48 koneč.

[15] HTTP – *HyperText Transfer Protocol* je hlavní metoda pro přenos informací na webu a protokol pro výměnu hypertextu a grafických, zvukových a jiných multimediálních obsahů na webu. Všechny definice protokolů podle iSlovar.

[16] SMTP – *Simple Mail Transfer Protocol* je internetový standard pro přenos elektronické pošty.

[17] TCP – *Transmission Control Protocol* je spojovací protokol přepravní vrstvy v souboru protokolů TCP/IP.

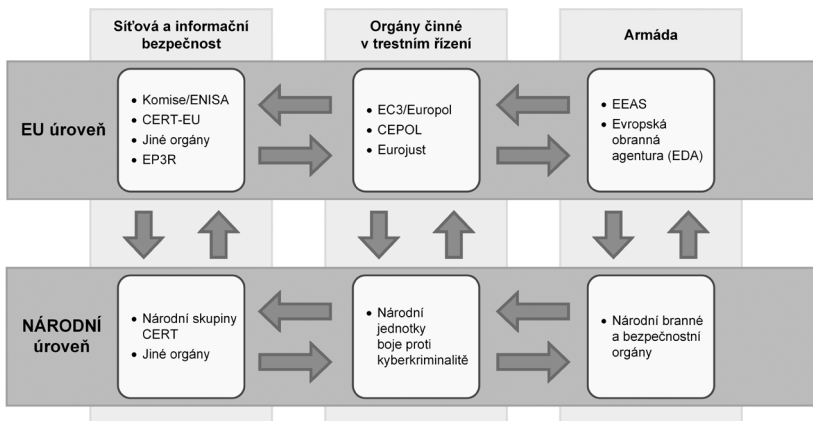
[18] UDP – *User Datagram Protocol* je nespojovací protokol přepravní vrstvy v souboru protokolů TCP/IP.

[19] PPP – *Point to Point Protocol* je protokol pro přenos dat, zpravidla používaný k vytvoření přímého spojení mezi dvěma síťovými uzly.

Pojem kybernetické bezpečnosti v širším slova smyslu se může týkat každé z těchto vrstev, proto ji lze chápat jako (Doria, 2007): (1) bezpečnost internetových protokolů, kde se jedná o objekty ochrany, které má na starosti IETF (*internet engineering task force*), (2) bezpečnost sítě, kterou chrání skupina CERT (*computer emergency response team*), (3) bezpečnost obchodování na internetu, která chrání zájmy firem (například bezpečnost elektronických bankovních služeb), (4) bezpečnost státní suverenity a národních zájmů, s níž je spojen pojem kybernetické války a kyberterorismu a (5) bezpečnost jednotlivce, respektive jeho základních lidských práv a svobod (například informačního soukromí).

Kybernetická bezpečnost v širším smyslu zahrnuje tři základní pilíře: (1) zajištění síťové a informační bezpečnosti (VOI), (2) činnost orgánů činných v trestním řízení a (3) činnost obranných sil (viz obrázek 4).

Obrázek 4: Pilíře zajišťování kybernetické bezpečnosti na evropské a národní úrovni[20]



Legenda:

- CEPOL – *European Police College*; Evropská policejní akademie
- CERT – *Computer Emergency Response Team*; Skupina pro vyřizování incidentů v oblasti bezpečnosti elektronických sítí a informací
- EC3 – *European Cybercrime Centre*; Evropské centrum pro boj proti kyberkriminalitě při Evropském policejním úřadu
- EDA – *European Defence Agency;* Evropská obranná agentura
- EEAS – *European External Action Service*; Evropská služba pro vnější činnost
- ENISA – *European Union Agency for Network and Information Security*; Evropská agentura pro bezpečnost sítí a informací
- EP3R – *European Public Private Partnership for Resilience*; Evropské partnerství veřejného a soukromého sektoru pro odolnost

[20] Evropská komise, 2013, s. 17.

- Eurojust – *The European Union's Judicial Cooperation Unit*; Úřad pro evropskou justiční spolupráci
- Europol – *The European Police Office*; Evropský policejní úřad

1.3 Kyberterorismus a kybernetické války

Kyberterorismus a kybernetické války (informační války; Bernik, Prislan, 2012)[21] jsou díky rozvoji internetu, do nějž se státy původně nevměšovaly, novější pojmy. V mezinárodních vztazích se za první vojenský kybernetický útok pokládá útok tamilských tygrů na Srí Lance roku 1997. USA přiznaly použití kybernetických zbraní již v době operací v Kosovu roku 1999 (Knight, 1999). Státy dnes vyvíjejí speciální zbraně pro kybernetické války (například program MonsterMind) (Zetter, 2014).[22] Oba pojmy jsou součástí nově definovaného kyberprostoru v okamžiku, kdy se stal životně důležitým pro existenci států a státních subsystémů (například bankovního, zdravotního nebo soudního). Pocházejí z doby po skončení studené války, kdy armáda hledala nový raison d'être: angažovanost v boji proti kriminalitě, později ve válce proti terorismu a v kyberprostoru. Právě kvůli angažovanosti v kyberprostoru se dnes hovoří o *remilitarizaci kybernetického prostoru* (Gagnon, 2008). Militarizace boje proti kriminalitě vedla spolu s remilitarizací kyberprostoru k problematickému rozlišování mezi kyberkriminalitou na straně jedné a kybernetickými válkami a terorismem na straně druhé (Ashenden, 2002).

Kybernetické války (Clarke, Knake, 2010) představují činy národních států nebo mezinárodních institucí, které napadají nebo se pokoušejí škodit kritické národní informační infrastruktuře (počítačům a sítím) jiných zemí. Jsou to tedy útoky v podobě škodlivých programů (angl. *malware*) nebo útoky DDoS prostřednictvím infikovaných počítačových sítí. Kybernetický terorismus pak označuje činy skupin, které se pokoušejí zničit, poškodit či změnit počítače, systémy nebo data. Jejich cílem je za použití počítačových síťových nástrojů znemožnit činnost kritické národní informační infrastruktury (například energetických nebo dopravních systémů), donutit nebo zastrašit vlády či civilní obyvatelstvo k určitým činům nebo ukončení některého konání. Terčem obou je kritická informační infrastruktura a počítačové systémy zapojené do internetu, rozdíl je však v subjektech působení (Libicki, 2009). Kybernetický útok musí splňovat některé podmínky, abychom jej mohli pokládat za čin (kybernetického) vojenského útoku.

[21] Bernik a Prislan kladou do popředí boj v souvislosti s informacemi, proto navrhují pojem informační boj: jedná se totiž o informace a o to, že pojem boj „zahrnuje nejen vojenské útočení, ale také obranu, vyzvědačskou a psychologickou činnost států, obchodních uskupení a občanských skupin" (Bernik, Prislan, 2012, s. 47).

[22] Program je schopen zaznamenat kybernetický útok na USA a samočinně vyvolat odvetná opatření.