BRAVE NEW DIGITAL WORLD

8. VYSOKÁ HRA PATRIOTŮ

ARCHEOLOGIE GEOPOLITIKY SÍTĚ

* V období průmyslové revoluce informace nabývají na významu – šíření informací přináší šíření inovací, emancipaci buržoazie, zefektivnění obchodu

* V rámci nových národních států vyvstává dilema jestli a nakolik tyto toky informací regulovat (např. emancipovaná společnost vs. konkurenční výhoda)

* Přenos informací ke správě impéria začíná využívat Francie a s příchodem telegrafu především Británie

GEOPOLITIKA SÍTĚ VE 20. STOL.

* Počítačová síť k vojenským a správním účelům
* Především řešena je ale otázka televizní a rozhlasové sítě
* V období studené války fungují rádiové rušičky a ponorky určené ke stříhání podmořských kabelů
* ČLR se v 70. letech staví do čela uskupení NWICO, která chce bojovat proti „kulturnímu imperialismu“

GEOPOLITIKA SÍTĚ VE 20. STOL.

* Na Západě je ustaven étos konektivity („David mikročipu porazí Goliáše totalitarismu“)

* Clintonova a Gorova administrativa spouští iniciativu Global Information Infrastructure, jejímž cílem je vytvořit „světovou komunitu“ umožněnou novými komunikacemi

* U. S. Telecomunication Training Institute, USAID a Světová banka finančně podporují růst internetu (v novém tisíciletí navazuje Digital Freedom Iniciative)

GEOPOLITIKA SÍTĚ VE 20. STOL.

* „Národ, který do svého hospodářství nejvíce zahrne vysoko-výkonnostní vypočítávání se velmi pravděpodobně vynoří jako dominantní intelektuální, ekonomická a technologická síla dalšího století.“ <Gore, 1991>

* V r. 1998 už ICTs představují 45 % amerického exportu

* Za připojení k americkým serverům se platí poplatky americkým síťovým firmám

WAR ON TERROR

* Nový způsob financování bezpečnostně orientovaných ICT projektů představuje In-Q-Tel (1999); CIA a NSA začínají vystupovat jako Venture Capital firma (toto později směruje i další subjekty)

* Po 9/11 takto spolu s novým Ministerstvem vnitřní bezpečnosti berou útokem „outlet technologických akcií," který vytvořila internetová horečka

* křemíkový trojúhelník, informačně průmyslový komplex; diskurz nové ekonomiky doplňuje diskurz sekuritizace

FREEDOM TO CONNECT

* Nová doktrína Hillary Clinton propaguje univerzální internetové připojení (návrat amalgámu neoliberální ekonomie a teorie veřejné sféry)

* Cenzura je legitimní pokud jde o ochranu autorského díla a nelegitimní pokud jde o hospodářství a politiku

* V měřítku mezinárodní interakce opět vyvstává spor o informační suverenitu

POLITICKÁ EKONOMIE INTERNETU

* Určitý institucionální řád pomáhá určitému fungování ekonomiky - je Freedom to Connect geopolitický nástroj k udržování tržní dominance?

* Eli Noam – zvyšování konektivity může rozevírat nůžky a to především mezi globálním severem a globálním jihem

* spor o fungování internetu stojí především jako správa v rámci ICANN vs. správa v rámci ITU

PROBLÉM MULTISTAKEHOLDERISMU

* Multistakeholderismus: kordinace soukromých a neziskových aktivit (event. i s vládami)

* ICANN: spravuje centrální adresář; ISOC: stará se o připojení třetího světa a spravuje doménu .org (její management pochází z korporátní sféry); IETF: vytváří standardy (Steering Group platí třetí strany)

* Je étos multistakeholderismu jen legitimizací? Americký a korporátní vs. nedemokratický bias?

SNOWDENOVA AFÉRA

* Freedom to Connect rétorika zmiňuje kyberprostor jako veřejný (sic!) prostor

* 2010: erozi soukromí ukazuje už roztržka mezi ČLR a Google či leaky na serveru Cryptome

* V roce 2012 (2013) kontraktor NSA Edward Snowden zveřejňuje informace o existenci mohutného sledovacího aparátu monitorujícího internet

SNOWDENOVA AFÉRA

* V rámci amerického Patriot Act a Foreign Intelligence Survaillance Act může např. NSA a FBI přistupovat ke komunikaci, kterou zprostředkovávají americké tech. společnosti (PRISM)

* Na tomto spolupracují především Microsoft, Facebook, Google a Yahoo!

* Kromě PRISM fungoval i MUSCULAR (historie vyhledávání) a kolem transatlantického datového kabelu vyvíjela své aktivity i britská GCHQ (za spolupráce s Vodafone)

SNOWDENOVA AFÉRA

* Poslušnost technologického sektoru jde odvozovat např. z narůstajícího objemu vládních a armádních zakázek

* Součástí práce NSA byla i rozsáhla lobbystická kampaň za oslabování šifrování

* Reakcí na tato a další odhalení je např. projekt BRICS Cable (datový kabel mimo americkou jurisdikci) či omezování bumerangového provozu Německem a Ruskem

MADE IN CHINA

* Nové jádro internetové populace leží zde, ČLR není dinosaurem, kterého světová síť zahubí

* Specifikem internetového provozu v zemi je nízký počet IXPs a „Velký čínký firewall“

* Vnitřní provoz na síti je monitorován a vnější usměrňován (inspekce paketů, blokace, zpomalování)

* Zodpovědnost za charakter provozu a jeho správu nesou provozovatelé; internet je zde privilegium ne právo

MADE IN CHINA

* K obcházení kontrolních mechanismů je používán Tor, Psiphon, VPNs či různé neologismy a jazykové kódy

* Naprostá majorita společnosti je ale s panujícím stavem spokojená (étos harmonie, důraz na společnost)

* Na síti (např. Weibo) je aplikován koncept ověřené identity, vláda země zaměstnává několik milionů opinionshaperů

MADE IN CHINA

* Čína je spojována s dlouhou řadou kyberbezpečnostních incidentů; hack služeb Google, kompromitace mailů tibetské exilové vlády, hack Skype, IBM, HP, Citigroup; průmyslová špionáž v Nortel, Lucent Technologies, Sun Microsystems, NEC Electronics, 3D-GEO, Lockheed-Martin

* Huawei a ZTE své technologie k regulaci internetového provozu prodávají řadě obskurních režimů.

* Ve velkých technologických firmách je zpravidla silně zastoupena Komunistická strana a Čínská lidová armáda

MADE IN CHINA

* Čínský síťový izolacionismus a regulace kyberprostoru jsou zároveň i ekonomickou strategií – početná domácí populace takto mohla vytvořit stabilní bázi pro tamní technologické společnosti.

* Každá ze známých služeb západních firem má v Číně svou domácí alternativu; Google – Baidu, Twitter – Sina Weibo, Facebook – Renren, YouTube – Youku, eBay – TaoBao, Netflix – Tencent Video, Twitch – Huya Live

* Čínská technologické firmy generují cca 30 % HDP země

ÍRÁN

* V roce 2009 zde dochází k rozsáhlým veřejným protestům organizovaným pomocí internetu

* 2010: sofistikovaný červ Stuxnet napadá centrifugy výzkumného nukleárního zařízení; 2012: nový rozsáhlý útok malwarem Flame (za oběma stojí USA a Izrael)

* Írán chce budovat vlastní relativně separovaný a monitorovaný „halal internet“

ARABSKÉ JARO

* Při nepokojích v Egyptě v r. 2011 dochází k úplnému odpojení internetových služeb, ekonomický dopad je vyčíslen na 18. mil dolarů za den

* Cute cat theory: omezení internetových služeb zasáhne všechny skupiny populace a vyvolá nepokoje – příklad Egypta toto potvrzuje

* Po pádu Mubarakova režimu je nalezeno množství dokumentů svědčících o spolupráci západních firem (Gamma Group, FinSpy) s egyptský bezpečnostním aparátem

ARABSKÉ JARO

* Během konfliktu v Sýrii internet fungoval běžně, první válka s rozšířením smartphonů

* Assadův režim konektivitu využívá ve svůj prospěch – monitoring komunikací (s pomocí západních firem), phishingové útoky na novináře z Al Jazzery, syrský disent a syrskou emigraci

* Dřívější metody vyhrazené kybernetickému zločinu úspěšně užívá stát