Rozhovory z konference IS2

Jeffrey Bardin

Informační války, propaganda a dezinformace

Jeff Bardin je profesionálem nejen na poli zpravodajské činnosti, ale i v oblasti informační bezpečnosti. Možná to bylo cílené a možná to je spíše z nouze ctnost. Při povaze činností, kterými se Jeff zabývá a kdy jeho protivníky jsou nebezpečné nepřátelské organizace jako například tzv. Islámský stát, či celé profesionální agentury cizích států, které pasou po jakékoli kybernetické chybičce z jeho strany, kterou by proti němu mohli využít, mu vlastně nic jiného než být kyberbezpečnostním expertem nezbývá. Vetšina Jeffových zákazníků trvá na naprosté anonymitě a diskrétnosti, nicméně úkolují ho tak, že získat jeho čas i jen na e-mailovou odpověď, je dosti náročná záležitost. Proto pro nás bylo opravdovým potěšením, když nás poctil svou návštěvou a mohli jsme jej uvítat na letošní konferenci IS2, kde prezentoval výstup z jednoho svého zpravodajského projektu.
Jeff je výkonným ředitelem a zároveň hlavním zpravodajcem ve firmě Treadstone71. Dříve pracoval v mamutích organizacích, jako jsou například General Electric nebo Lockheed Martin a ještě předtím sloužil v Americkém letectvu USAF jako kryptologický lingvista, kdy například v mnoha jazycích a pod mnoha kybernetickými identitami pronikal do nepřátelských skupin. Jeff též působil jako profesor v magisterských programech Kybernetická bezpečnost, Kontrarozvědka, Skrytá zpravodajská činnost a Počítačová trestná činnost a dnes nabízí školení a vzdělávání pro nejvyšší vedení firem i státních organizací. Toto jsou však jen vybrané střípky z jeho barvité kariéry nejen v oblasti informační bezpečnosti. Jeff Bardin poskytl u příležitosti svého vystoupení na IS2 pro časopis DSM exkluzivní rozhovor, kde odkrývá mnoho dalších zajímavých skutečností.

Máme svobodný přístup k informacím a veřejným médiím, kdokoliv s přístupem k internetu si může tato média číst. V případě USA je možné se takto dostat i k dříve utajovaným informacím na základě Freedom of Information Act. Do jaké míry myslíte, že je tento model svobodného toku informací funkční?

Myslím, že dříve byl úspěšnější než nyní, zejména protože vládní činitelé dnes obecně začínají být lehce nervózní z povahy informací, které jsou tímto způsobem zveřejňovány. Řekl bych, že je to vidět i v USA se současným prezidentem, který se snaží takovou svobodu informací omezit. A vidíte také další ve světě, kteří mají podobný pohled, často hraničící s autoritářstvím, jako například Erdogan v Turecku, Putin v Rusku - tam je to zcela běžné, ale také různá hnutí jako Le Penová ve Francii nebo Geert Wilders v Nizozemí. Takže si myslím, že je vidět odpor k této otevřenosti ve vládních sektorech, protože se vlastně takového toku svobodných

informací bojí. Na druhé straně si myslím, že bychom proti tomuto přístupu měli důrazně bojovat a zajistit, že uděláme vše pro to, aby se svobodný tok informací zachoval v co největší míře. Samozřejmě dokud to nebude ubližovat vládě, protože je to příliš citlivé, některé věci by neměly být zveřejněné, ale pokud chcete svobodnou a demokratickou společnost, pak je transparentnost vaší vlády a informací prostě nezbytná, je její nedílnou součástí.

Co si myslíte o dnešních médiích, do jaké míry jsou ovlivněná, je ještě možné médiím věřit?

Myslím, že ti, kteří jsou plně znalí a vyškolení v žurnalistice a plně vnímají nezbytnost objektivity jako součást své práce, to jsou ti, kterým můžete věřit. Musíte se podívat na jejich texty, analyzovat je, sledovat klíčová slova, fráze, žargon, být obezřetní vůči cílení na osoby bez podloženého základu, chybějící citace, fakta nebo doplňující informace. Musíte mít citace, musíte mít něco, co podporuje vaše teorie, musíte validovat své zdroje a validovat je jako reálné. Dneska lidé až moc často převezmou názor, jen protože mají určitý politický sklon, nebo jím sami chtějí něčeho dosáhnout. Tím pádem dostanete velmi subjektivní pohledy, protože na internetu kdokoliv může publikovat cokoliv. Bloger není žurnalista. A ten, kdo píše, musí validovat to, co píše, pokud to nedělá, pak musíte sami hodnotit autory na základě jejich kredibility, spolehlivosti a platnosti informací, které poskytují. Jestliže zjistíte, že to, co publikují, není validní, musíte je vyhodnotit jako nedůvěryhodný zdroj. Myslím si, že se toto prostředí dost znepřehlednilo rozličnými organizacemi, které tlačí propagandu, šum a informace, které publikují, protože za ně byli zaplaceni. Vzdálili jsme se od doby, byť ne tak nedávné, kdy noviny byly primárním zdrojem informací, doby, ve kterých lidé v televizi skutečně mluvili o zprávách, ne o názorech a mluvili o zprávách, ne o pocitech. Protože pocit není fakt. A to je jeden z problémů, které máme. Musíme se vrátit zpátky k faktům. Pokud najdeme média typu Breitbart nebo Fox News, které publikují nepravdivé informace pravidelně, musíme je hodnotit, validovat a jít za to po nich. Pokud je lidé chtějí sledovat, ať je sledují, ale musí pochopit, že to nejsou zprávy, ale televizní show. Vrátit se zpátky k základům, tedy validování zdrojů, je klíčem. Další problém, který máme, jsou memy (odborně jednotka kulturní informace, v tomto kontextu obrázek vyjadřující myšlenku, emoci či situaci, často s komentářem - pozn. red.) či spíše inženýrství s ním spojené - čili vezmete obrázek, dáte k tomu slogan nebo text, který ale není pravdivý, dáte to na Facebook, Twitter a lidé to berou jako pravdu, jako skutečnost a pak to propagují napříč internetem. Berou to jako validní, protože chtějí, aby to byla pravda, říká se tomu konfirmační zkreslení. Tito lidé jsou pak vystaveni takzvané kognitivní disonanci - je jim prezentována nějaká informace, a protože je to rozrušuje, tak tomu nechtějí věřit, a přestože je to pravda, půjdou radši jinam, na jiný web, kde jsou informace, které jsou pro ně více vyhovující a které jsou v souladu s tím, čemu věří a co jim je příjemné. Vidíme, že pochopení psychologie lidí, pomáhá vládám s dezinformací a kamufláží. Příkladem budiž ruská maskirovka, kde na to mají celé programy, které se soustředí pouze na takové činnosti, viděli jsme to při volbách v USA, viděli jsme to s Angelou Merkelovou, ve Francii, v Nizozemí a toto bude pokračovat. Protože pro většinu lidí je snazší věřit něčemu, s čím jsou v souladu, než objevit tvrdou pravdu.

Když se na to podíváme z historického pohledu, kdy se začaly používat informace jako zbraně?

Od počátku časů, informace byly odjakživa využívány ke klamání, popírání, manipulaci, dezinformaci. Můžete jít až do dob prvních válek, klamali jste vašeho nepřítele, aby věřil něčemu, co není skutečné, například přemístěním vojáků tak, že budete mít výhodu manipulovat na bojišti. Toto se neustále dokola opakuje. To, co tu máme dnes, je instantní přístup k lidem. Média a různé jiné způsoby, kterými se dostávají informace k lidem, jsou bezprecedentní. Informace na dosah vašich prstů, čtyřiadvacet hodin denně sedm dní v týdnu, takže můžete manipulovat mnohem rychleji. Pohybuje se to velmi rychle, protože k tomu lidé mají neustále přístup, takže budou propagovat a šířit rychleji. Retweetování, repostování, odebírání, lajky a sociální sítě to jen umocňují. Takže když se vrátíme do dob, kdy byly války, viděli jsme to neustále, klamání a podvádění, vypadalo to, že zaútočíte nějak, ale zaútočil jste jinak. Také dezinformace v ekonomice jsou mnohem rychlejší, mnohem dynamičtější. Můžete manipulovat ceny akcií během okamžiku, stačí udělat komentář na sociálních sítích, když vám lidé věří, například když jste prezident USA a uděláte komentář o společnostech přemisťujících své zaměstnance do Mexika. Když toto oznámí na Twitter o oněch 140 znacích, akcie těch společností klesnou. Pokud byste věděl, že takové informace řekne, mohl byste spekulovat na pokles jejich ceny v krátkém prodeji a vydělat spousty peněz. A to je ekonomická válka, protože on ovlivní hodnotu akcií těchto firem a někdo na tom vydělá peníze. Akcie se časem vrátí nahoru, ale protože má takovou moc, málokdo si toto uvědomuje. Je tu mnoho kybernetických válek, z různé perspektivy bojiště, a ať už je to ekonomická, akademická, politická či jiná perspektiva, každá je dnes nějakým způsobem přítomna na internetu.

Zdá se mi, že se dokola to jádro problému opakuje, jen máme jiné nástroje, jsme v tom lepší a rychlejší.

Ano, a dotýká se to lidí, kteří se s ničím podobným nikdy nesetkali, v minulosti nečetli všechny noviny, nesledovali všechny zprávy a teď je můžete snadno ovlivnit i v místech jako například na venkově, kde dřív tato média nebyla.

Můžete v nich vzbudit zlost nebo pozměnit jejich vnímání. Máte dosah na mnohem větší počet lidí s více subjektivními zprávami a konstantním přívalem informací. Je to skvělé pro vlády, pokud chtějí manipulovat, a také to dělají. Souvisí to také s perspektivou totální války, kombinuje se to hybridně, fyzicky i kyberneticky. Můžu vás zmanipulovat, abyste udělal to, co chci a nepotřebuji ani vytáhnout zbraň. Vaše země zažila nedávno incident, kdy uniklo 7 000 emailů a dokumentů. To je o čem víte, předpokládáte, že to je to, co jste zachytili, ale pořád vám unikají všechny ty další střípky. Oni ukradnou takové informace, studují je a plánují nové kybernetické útoky nebo informační manipulace a pak to realizují. Takže je to sběr dat ze špionážní perspektivy, za účelem analýzy. Kdo jsi, co jsi, co děláš a jak se k tobě dostanu, jakou taktiku proti tobě mohou použít. Je to skenování, testování defenziv, krádež informací, aby se k vám mohli později dostat. Dělali jsme to v 2. světové válce, dělali jsme to fyzicky, kradli jsme plány a informace. Dnes, kdy nechráníme naše elektronické informace, jsou komukoliv na dosah ruky, a to doslova.

Jak si myslíte, že se ta situace bude vyvíjet během následujících let?

Z perspektivy informačních válek a kybernetiky obecně, budeme pokračovat v miniaturizaci a integraci internetu do všech aspektů našich životů. IoT, všechny věci budou mít přístup k internetu, auta už ho mají, jejich diagnostika už ho má, pak diagnostika na lidech - dáte do těla zařízení, které monitoruje vitální funkce, některé armády to už dělají. Poběží na tom váš domov, sledují se zvířata. Ve skandinávských zemích to už mají implantované v rukou pro přístup do budov. Takže víc a víc se to přesouvá „do nás“ a našich životů. Máte Alexu od Amazonu a Google Home, které ovládají vaše osvětlení, topení, elektřinu, nastavují bezpečnostní systém, otevírají dveře od garáže. Všechna tato zařízení obvykle dostanete naprosto nezabezpečená. Oni si prostě řeknou, nejdřív to prodáme a pak uvidíme, jestli se to bude dobře prodávat. Teprve po komerčním úspěchu řeší, jak to zabezpečit, protože chtějí nejdřív vydělat peníze. A tohle byl problém vždy, od dob, co existuje IT, bezpečnost byla vždy něco, na co se myslelo až v druhé řadě. Není to klíčová komponenta, na kterou se myslí při návrhu, a to bude vést k mnoha problémům, budeme mít fyzické následky, lidé budou umírat a bude to jen horší, dokud si neuvědomíme co je problém. Prozatím je to každodenní boj, informační válka, ať už jsou to vlády nebo organizace bojující o online nadvládu, sbírání informací nebo zabudování malwaru do systémů pro pozdější využití. To se nezmění, jen budou mít více příležitostí, více takových zařízení. Jakmile přijde válka, tak budou schopni omezit nepřítele deaktivací jeho technologií, ať už to bude malwarem, který tam dali předtím, nebo elektromagnetickým pulsem, kterým deaktivují elektrická zařízení i sítě. To by byl první krok, kterým naruší řízení, komunikaci a kontrolu. A bude to horší a horší, a to rychleji a rychleji. Věci se zrychlují exponenciálně, schopnost zakomponovat

technologie do lidí, domů, zařízení. Domy se začnou stavět od základů SMART, vaše zdravotní záznamy budou uložené ve vašem těle, budete mít otisk prstu a kód, dvoufaktorovou autentizaci k přístupu k vašim záznamům. Ale to bude možné manipulovat, eventuálně vás tím může někdo zabít, když např. automatické zařízení na dávkování inzulinu nebude fungovat korektně. Toto se bude zhoršovat, protože chceme vždycky nejdřív dolary a až pak bezpečnost. Bohužel se to doteď nezměnilo, vidím to od svých začátků, kdy jsem se tímto oborem začal zabývat. Bezpečnost je sekundární problém. A když se začne řešit pak, stojí to o to víc. Je to skoro jako stavět auto bez brzd. Líbí se vám to, je to fajn, ale potom si uvědomíte, že ty brzdy potřebujete, že potřebujete pásy, klaxon a musíte to dodělat. Pak se auto ale nechová jako v původním návrhu, špatně jede, zatáčí, stojí více peněz. Tyto nedostatky se následně svádí na bezpečnost, kdyby se s ní ale počítalo od návrhu, nikdy by nevznikly a místo toho by celé prostředí bylo funkční a bezpečné. Tak se to ale neděje. Jsem blazeovaný a naprosto zklamaný, že se toto od dob, co se tomu věnuji, stále nezměnilo, všude kudy chodím, vidím dokola opakovat to samé. A dělám to už celý život. To byl vlastně jeden z důvodů, proč jsem se přesunul z bezpečnosti do zpravodajství, kde jsem se specializoval původně. Mám to radši, než chodit někam a snažit se pomoci firmám s bezpečností, firmám kde CISO stále reportuje CIO, což je konflikt zájmů. To znamená, že jste už od začátku mrtví na příjmu, musíte bojovat, musíte změnit člověka, jehož infrastruktura je problém, člověka, který ovládá váš plat, vaše hodnocení, vaše zaměstnání. A to prostě nedává smysl.

Nezbývá mi než souhlasit, konzistentně se v ČR setkávám s tím, že organizace do bezpečnosti neinvestují proaktivně, ale v naprosté většině případů pouze, když musí a nezbývá jim nic jiného. Když si koupí obchodní software, vidí ten okamžitý přínos, ale když si

koupí bezpečnostní nástroj, není tam nic takového, ten jim nic nevydělá. Snad jen regulace nebo zákonné povinnosti v tomto něco změní, podobně jako to bylo s povinností zavedení např. bezpečnostních pásů do automobilů. Myslíte si, že regulace jako např. GDPR toto zlepší?

Možná, ale v autě máte fyzickou bezpečnost, ta mentalita je jasná. Teprve až někdo na dálku ve vozidle deaktivuje brzdy a způsobí něčí smrt, pak to teprve začneme brát vážně. Když jsem vyrůstal, neměli jsme pásy, mohli jsme sedět na korbě, stát, nikdo to neřešil, ale lidi se začali zraňovat, tak pojišťovny začaly řešit, jak tomu zamezit a objevily se bezpečnostní pásy. Vzpomínám si, že když se poprvé objevily, tak tomu lidé odporovali, nechtěli je používat. A to je perfektní příklad, aby se takové věci prosadily, musíte lidi nechat s tím vyrůstat. Dnes to nikdo neřeší, všichni sdílí vše online, vyrůstají v tom, ale špatně, nejsou informování, neuvědomují si, že vše co zveřejní, tam navždy zůstane a nelze to vrátit zpět. Ať už je to obrázek, nebo něco, co řeknete, co by mohlo být nevhodné, bude tam navždy. Lidé si to neuvědomí, dokud například nevstoupí na trh práce a potenciální zaměstnavatel řekne, viděl jsem váš Facebook účet, pil jste, svlékal jste se, stávkoval jste. Můžete říct, ale já jsem byl mladý, na vysoké, ale oni vás stejně odmítnou. Nejde o to zakázat takové věci, ale o to, aby se lidé zajímali o bezpečnost už od malička, aby to bylo zabudované do jejich mentality. Své děti jsem od mala učil, nikdy nesdílejte své informace s nikým, koho neznáte, nepřidávejte si do přátel nebo nesledujte lidi, které neznáte. Dokonce jsem vytvořil hadrové panáky s lokátory, říkal jsem jim, že je budu sledovat, když budou ve škole. A snažil jsem se je nachytat, aby si mě přidali mezi přátele nebo mě sledovali na Facebooku a nikdy to neudělali. To bylo výborné, ale háček byl v tom, že všichni jejich přátelé se nachytat nechali. Takže díky tomu jsem byl schopný vidět, co dělají online skrz jejich profily. A upozorňoval jsem je na to, že to udělám. Řekl jsem jim, že udělali skvělou práci, ale problém je v tom, že všichni jejich přátelé se nachytali a skrz ně jsem byl schopný přijít na to, kam chodí na párty, jestli pijí jako nezletilí, jestli byli na místech, kde neměli být, když řekli, že budou jinde. Když jsem byl mladý, nebylo nic, čím byste mě mohli sledovat, neměli jsme ani telefony, mohli jsme jít kamkoliv, nikdo o vás nevěděl, kde jste. Dnes můžete být sledováni geolokací, co dáváte na web, co říkáte, co děláte, co vaši přátelé dělají, je to všechno venku. Potřebujeme mít otevřený a svobodný přístup, ale potřebujeme zároveň, aby lidi věděli, co dělají. Aby pochopili následky toho, co dělají online. Doufejme, že se stane něco, co nezpůsobí smrt lidí, ale donutí lidi jednat. Jen nevím, co ještě by se mohlo stát, už se ukradly miliardy datových záznamů, ale stále jsme se nezměnili...

Děkujeme za rozhovor.
Ptal se Pavel Krátký.