Civilne žrtve kibernetičkog rata

Nakon Sjeverne Koreje, koja je razvila vlastiti Linux, i Kina je odlučila krenuti istim putem. Njihova vojska ne želi više koristiti MS Windowse, smatraju ih sigurnosnom ugrozom. Nije jasno da li će rješenje biti inačica Linuxa, ili operacijski sustav razvijen ab ovo. U svakom slučaju, Kina ima dovoljno snage za takav poduhvat. Sjećamo se kako su Rusi kao uvjet prihvaćanja MS Windowsa tražili njihov izvorni kod. Čemu tolika sumnjičavost prema softveru?

O tome piše ZDNET [1]: Zahvaljujući zviždačima poput Snowdena, koji su otkrili da Amerikanci imaju velik arsenal alata za provaljivanje na računala, od pametnih televizora do Linux servera, routera, telefona, operacijskih sustava za stolna računala itd., Kinezi su se odabirom izrade vlastitog operacijskog sustava odlučili za princip security by obscurity.

Internet više nije samo mreža računala, mreža (dobronamjernih) ljudi koji se druže i pomažu jedni drugima, a uz to još i ogromna biblioteka dostupna svima (mreža informacija). Postao je tržište na kojem se kupuje i prodaje, tvrtke špijuniraju konkurenciju, medij za globalni marketing, raj za kriminalce koji pecaju naivce širom svijeta, ali i bojno polje na kojem se iskušavaju nove tehnike ratovanja. Slogan današnjih generala glasi: "Prije nego vojnička čizma stane na neki teritorij, rat treba dobiti u informacijskom prostoru." To ima višestruko značenje. S jedne strane treba prikupiti što više informacija o protivniku, kako se ne bi ulijetalo u nepoznato i kako bi se što bolje isplanirao napad na ključne ciljeve. S druge strane pažljivim plasiranjem informacija treba što veći broj ljudi, na svim stranama, uvjeriti u ispravnost vlastitih namjera i postupaka. Stoga nam, ako želimo misliti vlastitom glavom, ne preostaje drugo nego da svaku vijest odvagnemo prije nego je prihvatimo zdravo za gotovo. Čiji je interes skriven iza objavljivanja neke vijesti? Samo mali broj činjenica dospije u medije kao vijest, time one koje su odabrane kao pogodne za objavljivanje dobivaju dodatne slojeve značenja koje treba otkriti i osvijestiti. Dok bezazleno surfamo webom, upijajući ono što smatramo znanjem, za nas se lijepe nevidljive niti paučine iz mreže nečijih interesa.

Sve je veći broj država koje u okviru vojske osnivaju jedinice za kibernetičko ratovanje. Podatke o tome možemo naći u izvještaju Ujedinjenih nacija, dostupnom ovdje [2]. UN se trudi postići razoružanje i miroljubivu koegzistenciju. Ali logika podijeljenog svijeta nameće utrku u naoružanju: ako drugi imaju takva oružja, onda ih i mi moramo nabaviti.

Ne postoji jedinstvena definicija kibernetičkog ratovanja. Uglavnom se pod time misli na hakiranje, napad na računala protivničke strane, da se pribave povjerljivi podaci ili izazove nered, prekine normalno funkcioniranje druge strane. Ovakvim se napadima ne služe samo države, već i kompanije, teroristi, kriminalci, društveni aktivisti i slične grupe koje žele ostvariti svoje interese. Neki stručnjaci tvrde da je termin cyber war pogrešan, jer se tu ne radi o pravom ratu, nasilju. Naprotiv, cyber war trebao bi biti bez ljudskih žrtava. Mada postoji primjer miješanja kibernetičkog napada i primjene sile: u svibnju 2019 Izrael je bombardirao zgradu iz koje se upravo odvijao kibernetički napad.

U svim dosadašnjim ratovima stradavali su civili, možda najviše u prvom i drugom svjetskom ratu. Sjećamo se bombardiranja kojima su sravnjene cijele gradske četvrti (carpet bombing) i atomskih bombi bačenih na dva grada u Japanu. Današnja su oružja zahvaljujući novim tehnologijama preciznija, mogu se usmjeriti na vojne ciljeve i smanjiti civilne žrtve. Da li je taj princip primjenjiv i u kibernetičkom ratovanju? Kako bi uopće izgledale žrtve takvog rata? Da bi to razumjeli, moramo shvatiti što je sve cyber war.

Nedavna povijest nudi nekoliko primjera: napad na Estoniju [3] , kada su stručnjaci NATO saveza pomagali Estoncima da se obrane, ili napad na Iranska postrojenja za preradu radioaktivnog materijala, izvedena pomoću crva Stuxnet. Pada nam na pamet i jedna aktualna kriza: u sklopu akcije rušenja nepoćudnog režima u Venezueli nestalo je struje. Iako mediji ne spominju uzroke (o tome ćemo možda čitati za koju godinu), čini se da se radi o koordiniranom nastojanju da se narodu pokaže kako se njihova vlada nije u stanju brinuti za vlastiti narod, kako bi izazvali revolt i svrgavanje vlasti. Narod Venezuele gladuje, nema lijekova, tu sigurno ima kolateralnih civilnih žrtava.

Kad govore o kibernetičkom ratu vlade objašnjavaju da se radi o zaštiti vlastite kritične infrastrukture od napada izvana, smanjivanju ranjivosti, minimiziranju štete i skraćivanju oporavka od cyber napada. O ofenzivnim sposobnostima se nerado govori. Među njih spada špijuniranje (Snowden nam je otkrio masovno prisluškivanje koje provodi NSA, bez znanja država i građana koje se prisluškuje), sabotaže (napadi na električnu mrežu i ostale javne usluge, transport, satelite, odabrana industrijska postrojenja...), propaganda (fake news, korištenje društvenih mreža za psihološki rat), slabljenje protivnikove ekonomije (primjer su napadi virusa WannaCry i Petya na britanski zdravstveni sustav, farmaceutsku tvrtku i kaos koji su izazvali u Ukrajini).

Srećom, nije sva moć u rukama vojske, politike, velikih tvrtki, kriminala. U demokratskim društvima postoje i orgranizacije koje brinu za javni interes i prava pojedinca. Tako je nedavno održan skup na kojem su stručnjaci raspravljali o potencijalnim civilnim žrtvama kibenetičkog sukobljavanja. Sažetak je dostupan na stranicama Crvenog križa [4], Među primjerima navode ranjivosti medicinske opreme koja je sve više spojena na mrežu kako bi se omogućio udaljeni nadzor. Spominju pacemakere i inzulinske pumpe, opremu koja održava na životu pacijente. Jesu li proizvođači te opreme unaprijed razmišljali kako ti uređaji mogu biti mete napada i ugradili u njih sigurnosne funkcije? Civile će ugroziti i napad na ICS (industrijske kontrolne sustave) računala koja upravljaju javnim servisima poput električne i vodovodne mreže.

Za napade se obilno koristi malware, reverznim inženjeringom otkriva se njegov način rada i stvaraju nove inačice, za posebne namjene. Zamislimo situaciju u kojoj se atentat želi napraviti napadom na pacemaker određene osobe. Hoće li virus biti u stanju ciljano opstruirati jedan određeni uređaj, ili će stradati svi pacijenti koji ga koriste? Svijet je sve više premrežen uređajima spojenim na Internet koji su odreda potencijalne mete napada. IoT će još više povećati rizik.

Bilo bi sjajno kada bi se sve otkrivene ranjivosti objavljivale, a proizvođači brzo otklanjali sigurnosne propuste. No mnogi se neće držati tog principa, želeći ostvariti neku korist ili prednost. Ako otkrijete na primjer ranjivost softvera koji upravlja dronovima, hoćete li je obznaniti svima ili ćete je zadržati za sebe, kako bi je iskoristili u slučaju potrebe?

Kažu da na jednom stećku u BiH piše: "Stah, boga moleć, zla ne misleć. Ovden ubi me grom!" U današnjoj vojno-političkoj terminologiji rekli bismo da je bogumil kojeg je pogodio grom iz vedra neba kolateralna žrtva. Bogumili su vjerovali u kozmički dualizam, svijetom upravljaju istovremeno dobri i zli bog. Nije dovoljno biti pobožan, vjerovati u dobro i ne činiti zlo, svejedno te neka nasumična nepogoda može zbrisati s ovog svijeta. Današnje vjere dobro pripisuju Bogu, a zlo slobodi izbora koja je ostavljena čovjeku. No dualistički način razmišljanja još je sveprisutan. Pa zar se svi populizmi ne mogu svesti na jednostavnu formulu: mi smo dobri, oni drugačiji od nas su zli. Za sve naše probleme krivi su stranci, imigranti, susjedni narodi...

Sve dok se na taj način razmišlja i djeluje, dok postojimo "mi" i "oni", dotad će se svi odreda truditi da "naše" mreže i uređaji budu sigurni, a "njihovi" nesigurni, kako bi "mi" imali predost. Hoćemo li dočekati vrijeme kad će čovječanstvo shvatiti da smo svi "mi", i da ćemo biti sigurni jedino ako svi budemo sigurni? Ujedinjene nacije i Europska Unija primjeri su da je to ispravan put, usprkos svim pokušajima njihove destabilizacije i marginalizacije dugoročno će čovječanstvo evoluirati u tom smjeru. Barem se tome nadamo, a možemo i sami doprinijeti pazeći na to što mislimo, govorimo, kako djelujemo. Defetizam i cinizam, osjećaj nemoći pred silom, sve to samo održava postojeće stanje.

čet, 2019-06-13 22:49 - Aco Dmitrović**Kategorije:** Kolumna [5]
Vote: 0

No votes yet

story_tag: cyber war [6]
civilne žrtve [7]

Source URL: https://sysportal.carnet.hr/node/1849

Links
[1] https://www.zdnet.com/article/chinese-military-to-replace-windows-os-amid-fears-of-us-hacking/%20
[2] http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
[3] https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia%202017
[4] https://blogs.icrc.org/law-and-policy/2019/05/29/potential-human-costs-cyber-operations-key-icrc-takeaways-discussion-tech-experts/
[5] https://sysportal.carnet.hr/taxonomy/term/71
[6] https://sysportal.carnet.hr/taxonomy/term/326
[7] https://sysportal.carnet.hr/taxonomy/term/327