

Sajber rat

Vukotic Luka 120/2019

Matematički fakultet Beograd
Racunarstvo i društvo 2022
Profesor: Sana Stojanovic Djurdjevic

Uvod

- Sajber rat se odvija u sajber-prostoru koga cine sve racunarske mreze na svetu
- Kako je ova pretnja relativno nova veoma je tesko predvideti forme njenog daljeg razvoja i potencijalne nacine iskazivanja
- Sajber rat moze ukljucivati i kineticke i nekineticke aktivnosti



Sta je sajber rat?

- Predlagano je nekoliko definicija ali nijedna nije medjunarodno prihvacena
- Talinski prirucnik definise sajber rat kao sajber napad, u odbranbenoj ili napadnoj sajber operaciji, koji rezultuje u nasilju, smrti i/ili destrukciji
- DCAF definise sajber rat kao ratno ponasanje koje se sprovodi u virtuelnom svetu koristeći informacije, komunikacionu tehnologiju i mreze, sa namerom da poremeti ili unisti neprijateljske informacione i komunikacione sisteme

Ucestalost sajber napada

- U praksi nije moguće otkriti sve sajber napade koji se dogode iz više razlicitih razloga: neki su kratki ali ne ostavljaju tragove za sobom, neki se odvijaju godinama a da nisu otkriveni...
- Nemacka kompanija za telekomunikacije (DTAG) je uspostavila mrežu senzora koji služe kao rano upozorenje u slučaju sajber napada
- Samim razvijanjem tehnologije povećava se i broj sajber napada ali se također i povećava kvalitet odbrambenog sistema protiv sajber napada

Table I
Top 15 Source Countries for Cyberattacks in
May 2013 [5]

Source of Attack	Number of Attacks
Russian Federation	1 153 032
United States	867 933
Germany	831 218
Taiwan	764 141
Bulgaria	358 505
Hungary	271 949
Poland	269 626
China, The Peoples' Republic of	254 221
Italy	205 196
Argentina	167 379
Romania	153 894
Venezuela, Bolivarian Republic of	140 559
Brazil	140 281
Colombia	124 851
Australia	120 157

TOP 20 COUNTRIES BEST PREPARED AGAINST CYBER ATTACKS

RANKING OF CYBER SECURITY COMMITMENT AND PREPAREDNESS



Source: ABI Research/ITU

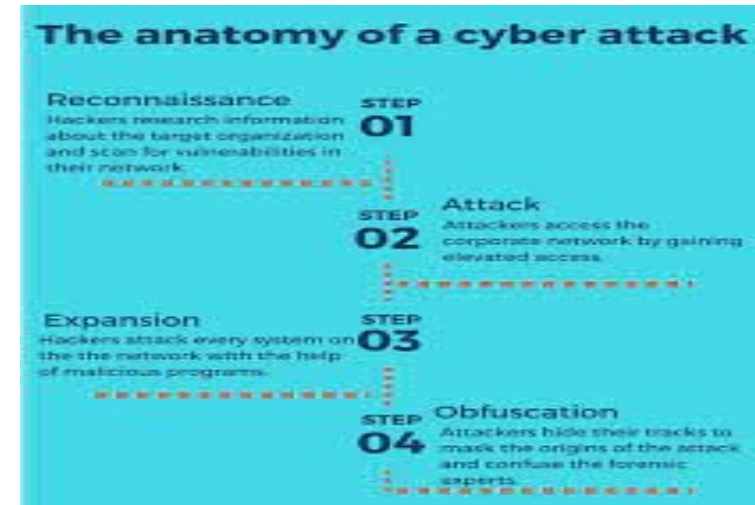
Zasto se javlja sajber rat?

- Naime, manje drzave ili neke teroristicke organizacije tradicionalnom vrstom ratovanja i upotrebom konvekcionalnih alata za ratovanje gotovo da nista ne mogu da urade protiv svetskih sila koje poseduju mnogo vise resursa u pogledu oruzja, novca...
- U okviru sajber rata/napada je mnogo priblizniji odnos snaga, potrebno je mnogo manje resursa, ali sa druge strane potrebna je povecana specijalizovana obuka



Kako se javlja sajber rat

- Sajber napadi koriste razne vektore, kako tehnoloske tako i organizacione
- Oni traze ranjivosti u bilo kom od entiteta koji cine sajber prostor
- Jedna od stvari koje su otkrivene je ta da je razlicita verovatnoca da napad odredjene vrste potekne iz odredjenim regionima



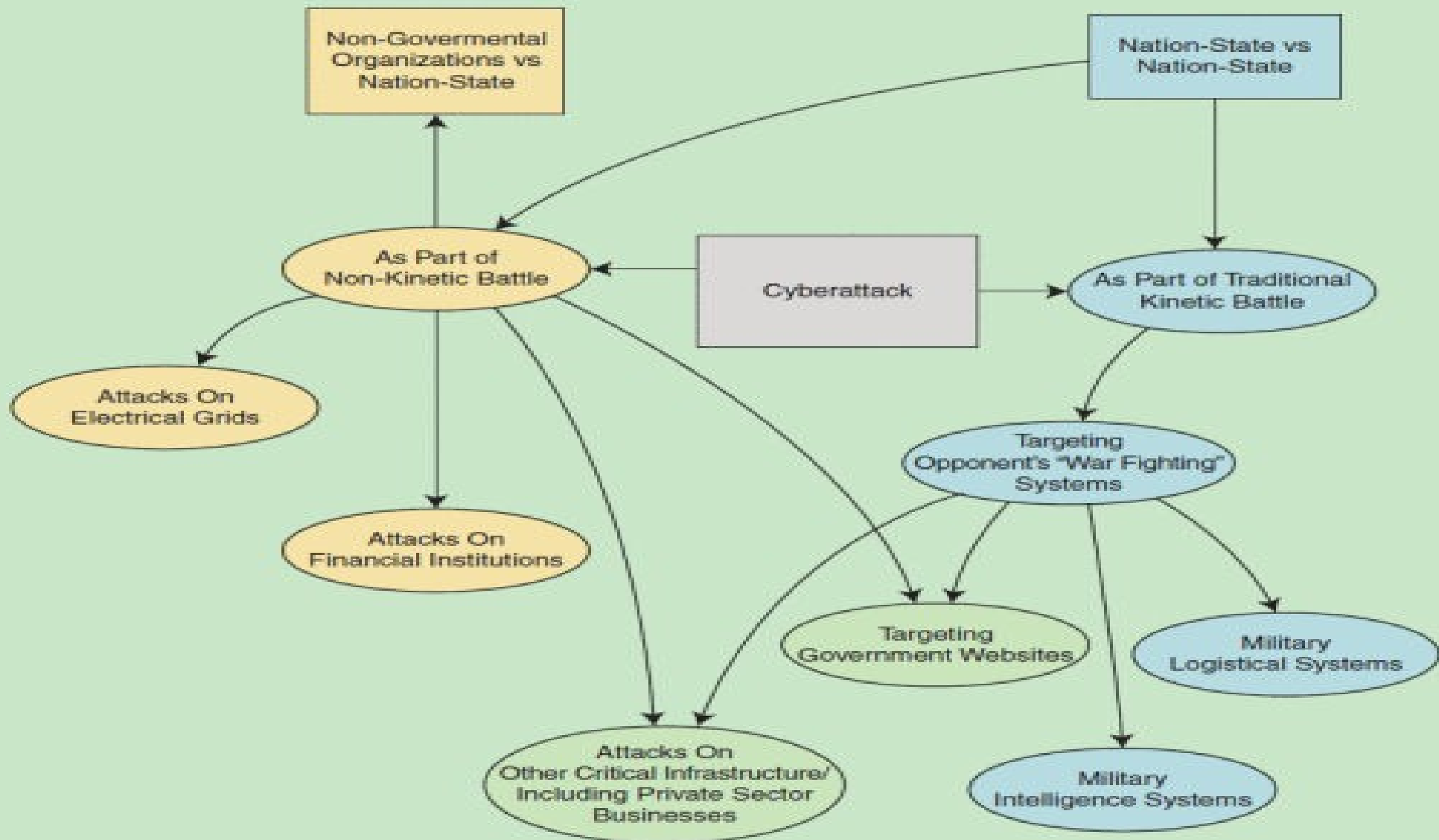
Metode napada u sajber prostoru

Table IV
Top 5 Attack Types in May 2013 [5]

Description	Number of Attacks
Attack on Server Message Block (SMB) protocol	5 970 973
Attack on Secure Shell (SSH) protocol	660 350
Honeytrap Attacker on Port 161	439 981
Attack on Port 5353	288 136
Attack on Netbios protocol	269 211

Klasifikacija sajber napada

- Sajber napadi se mogu pokretati na vise nivoa, a medju nivoima na kojima moze doci do sajber napada su:
 - Vlada naspram vlade
 - Asimetrično ratovanje: nedržavni akter protiv sopstvenih agencija ili dobavljača, ili druge vlade
 - Vlada protiv kritične infrastrukture druge vlade
 - Krivično nadahnuti hakeri naspram pojedinačnih korisnika



Types of Cyber Attacks



DoS and DDoS Attacks



MITM Attacks



Spear-phishing Attacks



Phishing Attacks



Whale-phishing Attacks

Najpoznatiji zabelezeni primeri sajber napada

- Dok je jos Rusija bila u satavu SSSR-a deo Trans-sibirskog gasovoda je eksplodirao. Naime malver je izazvao disfunkciju u SCADA sistemu koji je pokretao ceo gasovod
- Septembra 2010, Iran je napadnut Staksnet crvom, sa namerom da se specifcno pogodi nuklearno postrojenje Natanz. To je bio kompjuterski crv od svega 500 kilobajta koji je zarazio 14 industrijskih sajtova u Iranu, ukljucujuci i Natanz postrojenje
- U ratu protiv Hezbolaha 2006 godine, Izrael tvrdi da je doslo do sajber ratovanja tokom sukoba. Obavestajne sluzbe Oruzanih snaga Izraela su dosli do podataka da je nekoliko zemalja na Bliskom istoku unajmilo ruske hakere i naucnike da rade za njih

Pitanja?

- Sta je zapravo sajber rat?
- Da li je moguće otkriti sve sajber napade koji se dodgode?
- Koje klase sajber napada postoje?

Teme za diskusiju

- Da li ce se u buducnosti dogoditi da tehnologija vezana za odbranu od sajber napada bude razvijenija od same tehnologije vezane za napad?
- Koliko su razvijeni sistemi odbrane od sajber napada u Srbiji?

ATTACK SOURCES

- 0 Country
- 1 0 Japan
- 1 0 Romania
- 1 0 United States
- 1 0 Hong Kong

ATTACK TARGETS

- 0 Country
- 1 0 United States

Hvala na paznji!!!

ATTACKS

Timestamp	Description	Location	IP	Location	Source	Type
2016-06-06 10:10:10.00	Subprocess launched (cmd)	London, Romania	191.23.192.101	Washington, United States	191.23.192.101	cmd
2016-06-06 10:10:10.00	Regedit	London, Romania	191.23.192.101	Washington, United States	191.23.192.101	cmd
2016-06-06 10:10:10.00	File access	London, Romania	191.23.192.101	Washington, United States	191.23.192.101	cmd

ATTACK TYPES

0	Country	Port
1	0 microsoft	445
1	0 telnet	23
1	0 unknown	13501