Sajber rat

Vukotic Luka 120/2019

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 koristeci informacije, komunikacionu tehnologiju i mreze, sa namerom da poremeti ili unisti neprijateljske informacione i komunikacione sisteme

DCAF
Geneva Centre
for Security Sector
Governance

Ucestalost sajber napada

- U praksi nije moguce otkriti sve sajber napade koji se dogode iz vise 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 mrezu senzora koji sluze kao rano upozorenje u slucaju sajber napada
- Samim razvijanjem tehnologije povecava se i broj sajber napada ali se takodje i povecava kvalitet odbrambenog sistema protiv sajber napada

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

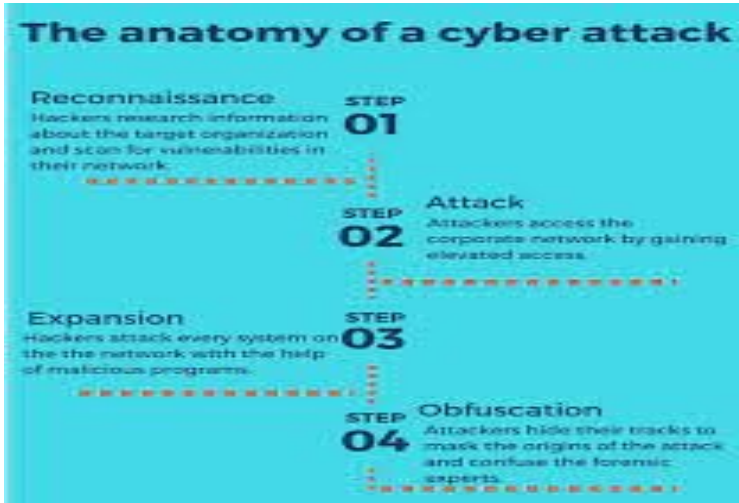
Source of Attack	Number of Attacks
Russian Federation	1 153 032
United States	867 933
Germany	831 218
Taiwan	764 141
Bulgaria	358 505
Hungary	271 949
Poland	269 626
China, The Peoples' Republic of	254 221
Italy	205 196
Argentina	167 379
Romania	153 894
Venezuela, Bolivarian Republic of	140 559
Brazil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

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 odredjenih 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

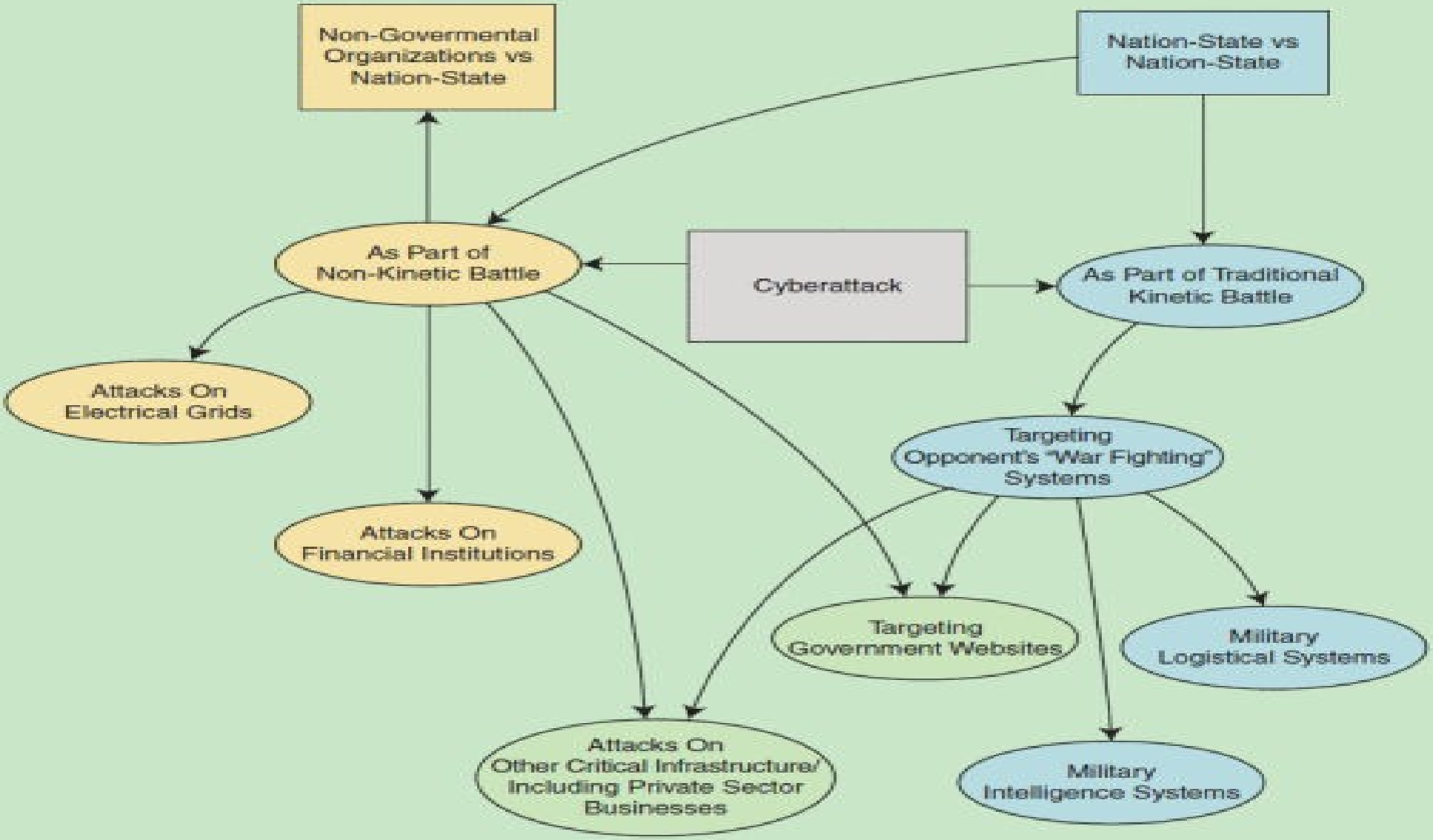
- Sajber napadi se mogu pokretati na vise nivoa, a medju nivoima na kojima moze doci do sajber napada su:

  - Vlada naspram vlade

  - Asimetricno ratovanje: nedrzavni akter protiv sopstvenih agencija ili dobavljaca, ili druge vlade

  - Vlada protiv kriticne infrastrukture druge vlade

  - Krivicno nadahnuti hakeri naspram pojedinacnih korisnika


Non-Governmental Organizations vs Nation-State
Nation-State vs Nation-State
As Part of Non-Kinetic Battle
Cyberattack
As Part of Traditional Kinetic Battle
Attacks On Electrical Grids
Attacks On Financial Institutions
Targeting Opponent's "War Fighting" Systems
Targeting Government Websites
Military Logistical Systems
Attacks On Other Critical Infrastructure/ Including Private Sector Businesses
Military Intelligence Systems

Types of Cyber Attacks

DoS and DDoS Attacks

Spear-phishing Attacks

MITM Attacks

Phishing Attacks

Whale-phishing Attacks

Najpoznatiji zabelezeni primeri sajber napada

- Dok je jos Rusija bila u sastavu SSSR-a deo Trans-sibirskog gasovoda je ekspolodirao. Naime malver je izazvao disfunkciju u SCADA sistemu koji je pokretao ceo gasovod
- Septembra 2010, Iran je napadnut Staksnet crvom, sa namerom da se specificno 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 moguce otkriti sve sajber napade koji se dogode?
- 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?


NORSE
Hvala na paznji!!!