BENCHMARKING CYBER OPS 2018

An initiative by

OnNet for OOAT

//UNCLASSIFIED

FOREIGN GOVERNMENT CYBER UNITS EXAMPLES

- ISRAEL = UNIT8200
- US = U.S. CYBERCOM, NSATAO, DHS NCCIC
- ISRAEL/US = “EQUATION GROUP” Name give by Kaspersky
- UK = GHCQ-JTRIG, NCSC, MYNOC
- SA = COMSEC
- Australia = ASD
- CANADA = CSEC
- CHINA = PLA61398
- NKOREA = LAZARUSGROUP
- RUSSIA = GRU6thDIR-FSO, GTsST
- IRAN = INCA
- DUTCH = JSCU

AFRICA

- Only cyber warfare unit known is under South African Government
- Owned under National Intelligence Agency NIA
- Formerly Electronic Communications Security ELS
- Interagency with OIC, Office of Interception Centre

EXAMPLES OF KNOWN NATION STATE CYBER WARFARE EVENTS

- Estonia cyber attack by Russia
- Crimea cyber attack by Russia
- Operation Olympic games by TAO and Unit8200 (EquationGroup) against IRAN
- Operation Nitro Zeus By TAO against IRAN by US
- Operation Socialite by JTRIG/MYNOC, done by UK
- Operation Rolling Thunder by JTRIG, operations by UK
- Ethiopian use of HackingTeam software RCS to spy on ESAT journalists and Activists
- Operation Aurora by Unit61398, operations in China
- Operation Disttrack by ICA, Operations in Tehran to respond to US
- Operation Turla Uroburos by Russian GRU6th Directorate in Russia
- Operation DarkHotel Unit61398, from Israel

EXAMPLES OF KNOWN NATION STATE CYBER WARFARE EVENTS

- Sony pictures attack by LazarusGroup responding to a movie potraying Nkorea Leader
- Red October – Unknown Nation State actor
- Operation Ghostnet by Unit61398 from China
- Operation NewsCaster by INCA in Tehran
- Operation Cleaver by INCA in Tehran
- Operation Shadow network by Unit61398 from China
- Operation Titan Rain by Unit61398 from China
- OPM attack by Unit61398 from China
- Kaspersky labs attack by Unit8200 from Jerusalem as a response on EquationGroup
- DNC attack by GRU6th Directorate/ GTsST
- Iran nuclear talks interception by Unit8200 as means of Israel covert Intel Collection
- IRAQ Surveillance State/Dragnet by TAO s321 to Intercept and apprehend Jihadis
- Dutch government cyber warfare team, JSCU hacked into a SVR safe house and goes after APT29 operators.

IDEAS

- Development of teams like Special Cyber Force Operators SCOs.
- Development of an Agency that can handle Cyber Warfare and Cyber Deterrence events.
- Big Data Analysis with Passive collections.
- Active Collection on targets, CNE to support SIGINT.
- Making Kenya the number one Cyber power in Africa.
- Information Collection and influence.
- Cyber Counter Intelligence on rival Nation State Cyber Actors.
- Counter Nation State cyber attacks against the country

MAJOR DOMESTIC THREAT ACTORS 2017

- ForkBombo group
- Anons
- Tizi group
- TellCode Team
- The Doctors