WEBINAR
Cybersecurity for e-diplomats: Hype and reality

Hosted by Diplo fellow
Vladimir Radunović
@vradunovic
Contents

Cyber-threats: cases, targets, motives, weapons
Response: militarisation vs. cooperation
Diplomacy: international cooperation, roles of stakeholders, actors and fora
Cyber-threats
Cases

Estonia

Cable-cut

Creeper

Stuxnet

„Aurora“
Targets

- **individuals** (ID, zombies)
- **business** (SMEs, banks)
- **government** (e-gov, databases)
- **public institutions** (databases)
- **core Internet infrastructure** (ISP, IXPs, fusion centers, data centers)
- **critical society infrastructure** (power/industry facilities, traffic, ...)
- **military assets**
Motives

- Hacktivism
- Crime
- Espionage
- Terrorism
- Warfare
Weapons and tools

Software flaws

Protocol flaws

Mind flaws

- Malware (viruses, trojans, worms)
- Bot-nets
- DDoS
- Social engineering (phishing, scams)
Botnets

Source: F-Secure
Botnets

Legend
- ATTACKER
- BOT HERDER
- ZOMBIE
- TARGET

Source: www.lessucettes.com
The Crimeware Economy

Crackers
- Vulnerabilities & techniques

Bot herders
- Computer power
- Data access

Fraudsters
- IP theft
- Customer IDs
- Employee IDs

DIPTLO
Militarisation

- **UN**: Expert group on international security in ICT
- **US**: 4x Cyber-Command with Pentagon
- **UK**: Defence cyber-operations group with defence ministry
- **Russia**: FSB (Federal Security Service)
- **China**: Cyber-warfare unit within PLA
- **Iran**: High council for cyber-space and cyber-defence command
- **NATO**: CCDCoE
- **EU**: European Defence Agency (EDA)
Cooperation

1. Critical Information Infrastructure Protection (CIIP) and network resilience
2. Legal frameworks and cooperation against cyber-crime
3. Defence and dialogue on IHL applications in cyberspace
4. Role of the corporate sector and Internet communities
5. Awareness building and developing institutional capacities
6. Internet governance and Internet diplomacy
Diplomacy
Complexity: Multidisciplinary
Complexity: Multistakeholder

"Too complicated..."
Complexity: Multistakeholder
Processes

- **CoE**: Convention on Cybercrime (2001)
- **ITU**: Global Cybersecurity Agenda (2008)
- **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)**: “Tallin Manual” (2013)
- **OECD**: Guidelines on Information Security
- **OSCE**: focus on cyberterrorism and Internet safety
- **G8**: Subgroup on High-Tech Crime on crime, terrorism and CIIP
- **Commonwealth**: Cybersecurity Initiative (2011)
- **Multilateral**: Group of Governmental Experts (US, Russia, China) on “International norms pertaining to state use of ICT” (since 2008)
- **Bilateral agreements**: US-China (2013)
Questions

Thank you for your time

Follow us on  www.diplomacy.edu
@igcbp @DiplomacyEdu @vradunovic