COUNT CYBERWEAPONS AND SAVE THE INTERNET

Towards Arms Control and Disarmament for Cyberspace

Thomas Reinhold, PEASEC

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Agenda

- **Why** is the task important?
- **What** are cyberweapons?
- **How** can cyberweapons get identified and controlled?
- **Next** steps towards cyber arms control?

Why is the task important?

- Ongoing militarization of the cyberspace
  - Big players, NATO and countries in Europe planing with offensive cyber capabilities
  - Problematic trending topics active/forward defense and hack back
  - Vulnerabilities of critical infrastructures
  - Mutual uncertainties and mistrust intensifies a cyber arms race
- Hold back information of vulnerabilities threatens everbody
- Constant activities undermine foreign IT systems
- Ambiguity of digital data and the risk of conflicts by mistake

Why is the task important? (2)

- Debates & initiatives on the peaceful development of the cyberspace
  - UN Group of Governmental Experts (UN GGE)
  - OSCE level
  - State and/or industry driven approaches
- For arms control the cyberspace is different & established approaches fail
- Many new technical questions and features require new solutions

What are cyberweapons?

- Missing official common understanding for the term "cyberweapon"
  - Analogy to the "use of force"
  - Usually interpreted as "serious harm of objects or people"
  - Assessment by intend and effects of incidents
- But: arms control need *ex ante* measurable parameters
- How to count bits and bytes?

How can cyberweapons get identified and controlled?

- Differentiating cyberweapons within spectrum of malware
- Indicators that distinguishes a cyberweapon
  - Means of propagation: from targeted and tailored to randomly spread
  - Controllability of the deployment: from fully manual to automated (see the LAWS debates)
  - Autonomy of payload evolvement and abilities to stop the payload
  - Quality of penetration measure (uniqueness and distribution of the vulnerability & exploits)
  - Quality assurance and prevention of unintended effects

➔ Indicators to asses a specific tool towards its "cyberweapon character"

How can cyberweapons get identified and controlled? (2)

- Classifying the potential impact of a cyberweapon
- Cyberweapons can work very differently in comparison to conventional weapons
- Dimensions to consider
  - Degree of possible direct damage of a cyberweapon
  - Spatial (how many) and temporal effects (how long)
  - Second level (directly connected systems) and third level (depended systems) effects
  - Intended and unintended effects

➔ Dimensions to classify cyberweapons by its entire potential effects

Next steps towards cyber arms control?

- Consent that all nations rely on the safety and integrity of the internet
- Commitment to IHL and rules of international behaviour in cyberspace
  e.g. the integrity of foreign IT systems
- Clear distinction between espionage and operations with malicious payload
- Agreements on limiting the (unintended) destructive effects of malicious code
  e.g. technical cooperation for the safeguard of exploits

Next steps towards cyber arms control? (2)

- Practical solutions reguired for potential regimes
  - Measure and classify the potential impact of cyberweapons
  - Cyber disarmament: Limit and reduce exploit stockpiles
  - Mutual control and Verification of cyberweapon arsenals
- Protection of civil cyberspace infrastructures
- It all starts with Confidence Building Measures (CBM)

Conclussion

- International definition of cyberweapons
- Agreements on limiting the (unintended) destructive effects of cyberweapons
- Development of technical procedures for measurement
- Stronger integration of the computer science community

Thanks

“The usual stuff — a new virus from the Joker, spyware from the Penguin, malicious code from Cat Woman, another phishing scheme from the Riddler.”

reinhold@peasec.de
twitter @cyberpeace1
cyber-peace.org