COUNTING CYBER WEAPONS

New Approaches to identify and control destructive cyber tools

Thomas Reinhold, PEASEC

PEASEC CYSEC Cybersecurity TU Darmstadt TECHNISCHE UNIVERSITÄT DARMSTADT

Agenda

- **Why** is the question important?
- **What** are destructive cyber tools?
- **How** can cyber weapons get identified and controlled?
- **Next** steps towards a necessary regulation?

Why is the question 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
- Debates & initiatives on the peaceful development of the cyberspace
- For arms control the cyberspace is different & established approaches fail
- Many new technical questions raise the necessity of IT security community integration

What are destructive cyber tools?

- Missing official common understanding for the term "cyber weapon"
    - Analogy of attacks with cyber weapons and its effects related 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
- Counting bits and bytes?

How can cyber weapons get identified and controlled?

- Disclaimer: Work in progress
- Differentiating cyber weapons within spectrum of malware
- Indicators that distinguishes a cyber weapon
  - Means op 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 handling prevention of unintended effects

➔ Indicators to asses a specific tool towards its "cyber weapon character"

How can cyber weapons get identified and controlled? (2)

- Classifying the potential impact of a cyber weapon
- Cyber weapons can work very differently in comparison to conventional weapons
- Dimensions to consider
  - Degree of possible direct damage of a cyber weapon
  - 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 cyber weapons by its entire potential effects

How can cyber weapons get identified and controlled? (3)

- Practically measurable parameters of cyber weapons
- "External" parameters without adjustments to existing IT systems
  - Power consumption and capacities of the power supply
  - Thermal performance of the cooling systems
  - Network bandwidths and maximum capacities
  - Amount and data rates of network connections
  - Amount of technical and administration staff

➔ Many parameters measurable by existing systems

➔ Suitable for monitoring the status quo of facilities

How can cyber weapons get identified and controlled? (4)

- "Internal" parameters with necessary adjustments on tools or infrastructures
  - Network connection metadata (who transmits what to whom and how often)
  - Usage of anonymization services
  - Detection of digital artifacts, exploits, and security vulnerabilities

  ➔ Monitoring the current application of systems

  ➔ Acceptance and political approval in question

  ➔ But: Probable unilateral measure for trust building

Next steps towards a necessary regulation?

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

Thanks

HONEST! RUSSIA HACKED MY COMPUTER AND STOLE MY HOMEWORK!
©2017 SUMMERS TRIBUNE CONTENT AGENCY

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

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

PEASEC

CYSEC Cybersecurity TU Darmstadt

CRISP Center for Research in Security and Privacy

TECHNISCHE UNIVERSITÄT DARMSTADT

IANUS SCIENCE · TECHNOLOGY · PEACE