Cyberspace and Warfare

Thomas Reinhold - reinhold@ifsh.de - cyber-peace.org

Institute for Peace Research and Security Policy Hamburg
Cyberspace and Warfare - Overview

• A little bit of context
• What is a cyber attack?
• The fuzziness of prediction with malware
• Problems for confidence and peace building measures in cyberspace
• Consequences and next steps
A little bit of context

- Stuxnet 2010 and its aftermath
  - Protagonists with "cyber arsenals"
  - Questions of own vulnerabilities and consequences for international security
- UNIDIR study 2013*
  - 47 states with military cyber programs
  - 10 states with dedicated offensive military orientation
- BMVg: New cyberspace policy
  - Specific cyber unit, centralisation of competences (~15,000 people)
  - Authorisation for offensive actions
- NATO
  - Tallinn-Manual and the rules of cyber attack
  - Cyberwar regular agenda item
  - Rapid task force

* United Nations Institute for Disarmament Research
What is a cyber attack

• Most of the malicious activities in cyberspace are cybercrime
  • Scope of law enforcement

• What if the protagonists are states?
  • Scope of humanitarian law and the law of armed conflicts

• What is the threshold between penetration and attack?
  • What is the equivalent of "armed attack" in terms of humanitarian law?

What is a cyber attack

Brown, G. D. & Tullos, O. W.
What is a cyber attack /2

• Binding and uniform definitions necessary for
  • Evaluation of concrete conflicts
    Something is a cyber weapon if its damage equals the damage of an armed attack as defined by the UN Charta Art. 51
  • Classifications for disarmament agreements, arms control and verification
  • To confine between defence and offense capabilities
  • Setting the threshold for dual use regulations
The fuzziness of prediction

- Fuzziness of prediction with malware:
  - How to estimate the vulnerabilities
  - How to estimate the necessary resources for a specific effect / damage
  - How to control and operate a released malware
  - How to specify what target they will hit (and which not)
  - How to estimate the chain effects of disrupted/destroyed IT systems
Problems for confidence and peace building measures

- Specific features of cyber weapons as problem for established concepts
  - Immaterial
  - Virtual
  - Easy to duplicate
  - No specific technical facilities necessary
  - Strong dual use character
  - Difficulties with attribution

<table>
<thead>
<tr>
<th>Measures</th>
<th>Elements</th>
<th>Applicable for Cyber Space?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographical</td>
<td>• Demilitarized Zones</td>
<td>• Not possible</td>
</tr>
<tr>
<td></td>
<td>• Thin-out Zones</td>
<td></td>
</tr>
<tr>
<td>Structural</td>
<td>• Defensive Orientation of Armed Forces</td>
<td>• Accept defense but prohibit offense?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>• Limits on Maneuvers and Exercises</td>
<td>• Prohibit offensive military exercises</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Declaratory</td>
<td>• No first Use</td>
<td>• Unilateral declarations</td>
</tr>
<tr>
<td>Verification</td>
<td>• Air- or space-based sensors</td>
<td>• unlikely</td>
</tr>
</tbody>
</table>

*Neuneck, G, "Confidence Building Measures - Application to the Cyber Domain", Lecture, 2012*
Consequences and next steps

- Vulnerability of important systems / critical infrastructures
- Effects and damages of malware are the key for their regulation
- Build up better defence, but avoid concerns about better offence
- Shaping the cyberspace as its a man made domain
- Raising the awareness
- Ban of cyber weapons
Thanks
Appendix A: Military cyber planning

• It's easy to vandalise random targets but hard(er) to hit a specific one
• Military planning differs highly from criminal planning
  • Identification of possible high quality strategic targets and their weaknesses
  • Need for undetected system flaws to gain access to the systems
  • Build up a persistence in the target systems to be ready in time
  • "1 or 2 till 5 years for planning time" (Felix Lindner, Security Labs)
• Cyber weapons aren't cheap
Appendix B: What are cyber weapons?

• What are cyber weapons and how to classify them?
  • By its technical specifications (directed, controllable, predictable use of force)
  • By the damage it cause (intended and unintended)
  • By the intention of its operators (who against whom, why, for what purpose)