

Working Group 3: Cyberspace and Warfare

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

Institute for Peace Research and Security Policy Hamburg

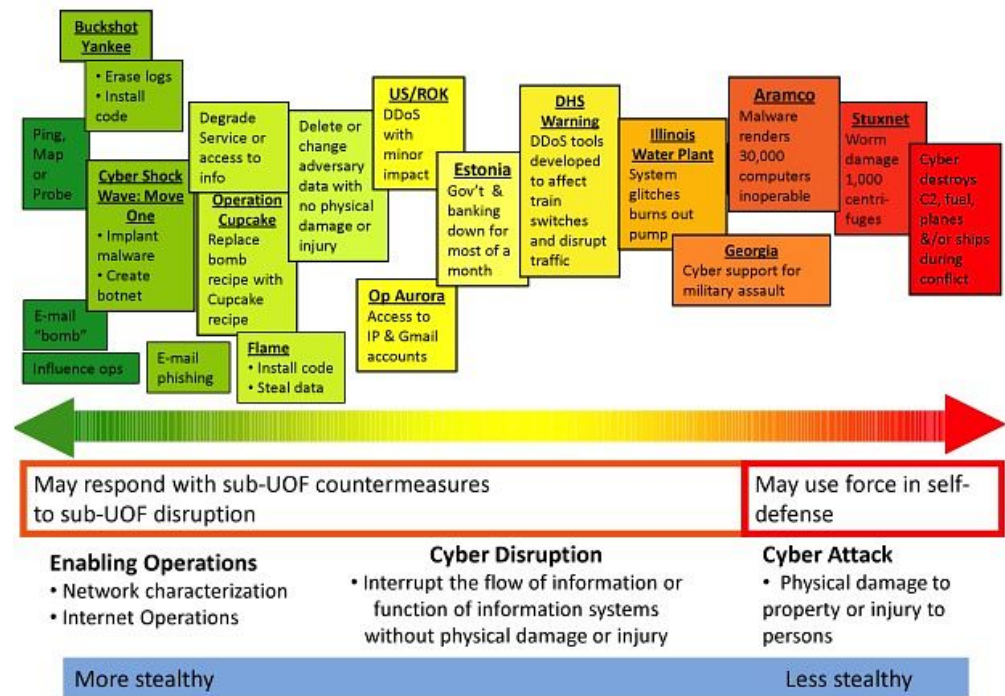
- A little bit of context
- What is a cyber attack?
- The fuzziness of prediction with malware
- Problems for confidence and peace building measures in cyberspace
- Consequences and next steps

- Stuxnet 2010 and its aftermath
 - Protagonists with "cyber arsenals"
 - Questions of own vulnerabilities
 - Consequences for international security
- UNIDIR study 2013*
 - 47 states with military cyber programs
 - 10 states with dedicated offensive military orientation

* United Nations Institute for Disarmament Research
"The Cyber Index - International Security Trends and Realities", Geneva, 2013

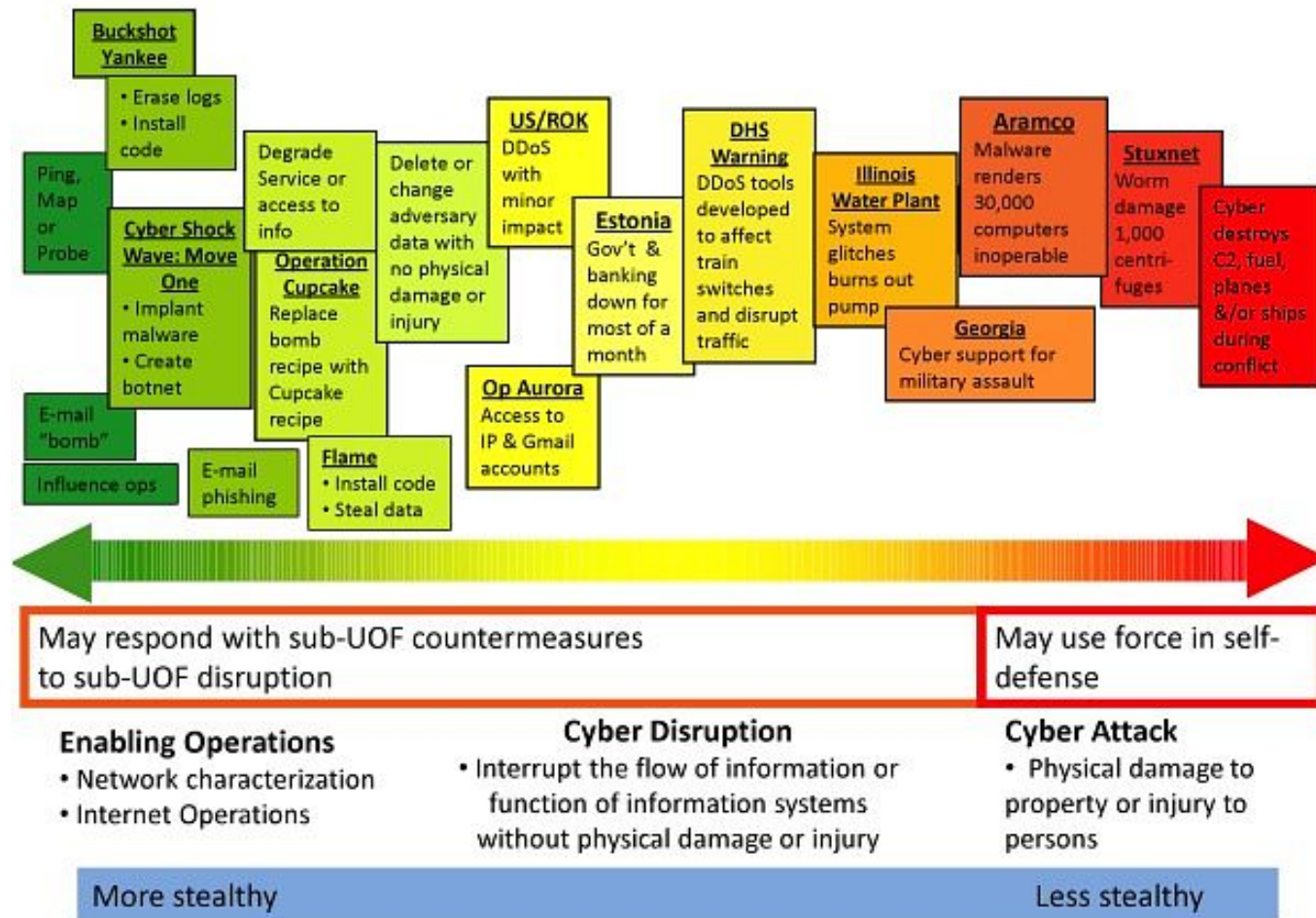
What is a cyber attack

- 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?



Brown, G. D. & Tullos, O. W.
"On the Spectrum of Cyberspace Operations", Small Wars Journal, 2012

What is a cyber attack



Brown, G. D. & Tullos, O. W.
"On the Spectrum of Cyberspace Operations", Small Wars Journal, 2012

- 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

- 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

- 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

| Measures | Elements | Applicable for Cyber Space? |
|--------------|--|---|
| Geographical | <ul style="list-style-type: none">• Demilitarized Zones• Thin-out Zones | <ul style="list-style-type: none">• Not possible |
| Structural | <ul style="list-style-type: none">• Defensive Orientation of Armed Forces | <ul style="list-style-type: none">• Accept defense but prohibit offense? |
| Operational | <ul style="list-style-type: none">• Limits on Maneuvers and Exercises | <ul style="list-style-type: none">• Prohibit offensive military exercises |
| Declaratory | <ul style="list-style-type: none">• No first Use | <ul style="list-style-type: none">• Unilateral declarations |
| Verification | <ul style="list-style-type: none">• Air- or space-based sensors | <ul style="list-style-type: none">• unlikely |

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

- 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



- Its easy to vandalise random targets but hard(er) to hit a specific one
- Military planing differs highly from criminal planing
 - 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, Recurity Labs)
 - Cyber weapons aren't cheap

- What are cyber weapons and how to classify them?
 - By its technical specifications (directed, controlable, 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)