Nations states and military activities in cyberspace

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

Institute for Peace Research and Security Policy Hamburg

A little bit of context

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Stuxnet 2010 and its aftermath
  - Protagonists with "cyber weapons arsenal"
  - Consequences for international security
- UNIDIR study 2013*
  - 47 states with military cyber programs
  - 10 states with dedicated offensive orientation
- NATO
  - Cyber attacks part of collective defence
  - Can raise article 5 of treaty
- New cyber strategy of the German federal ministry of defence
  - Establishing a new (possibly offensive) department for cyber capabilities

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

Technological trends

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Computers everywhere
  - Automating (e.g. traffic control)
  - Centralisation (e.g. insurance database, health system...)
  - Digitalisation (e.g. elections, landline communication systems)
  - Optimisation (e.g. high speed stock exchange trading)
- Dependencies of IT services and infrastructure
  - Critical infrastructure
  - Governmental and federal services and administration
  - Civil communication
  - Basically all military systems
  - ...

The challenge of cyber security

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Security is always a fight against superior opponents
  - IT as an "easy" target
  - Necessity of connected services
  - Rapid technological progress vs. slow decision processes
  - Balancing available resources and the scope of protection
- The NSA and the reality of "omnipotent" attacker

The challenge of cyber security

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Security is always a fight against superior opponents
  - IT as an "easy" target
  - Necessity of connected services
  - Rapid technological progress vs. slow decision processes
  - Balancing available resources and the scope of protectionThe NSA and the reality of "omnipotent" attacker

- Cyber security - the obvious concepts
  - Connecting the stakeholder
  - Capacity building and technological modernization
  - National obligation to report incidents
  - Incident sharing (CERTs)
  - Fostering the IT security research

Cyber security of nation states

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Security of nation states
  - Internal security => Legislation and law enforcement
  - External security => Diplomacy, international treaties and military forces

- International offensive actors in cyberspace exist, **but**
  - Currently no common definitions for cyberspace / cyber attack / ...
  - Just a few actors dominate most the technology
  - Diversity of potential actors
  - Costs of cyber attacks cheaper than "boots on the ground"
  - Many traditional security concepts and measures won't work for cyberspace

Confidence and security building measures in cyberspace

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Established measures vs. cyberspace

Measures	Elements	Applicable for Cyber Space?
Geographical	• Demilitarized Zones • Thin-out Zones	
Structural	• Defensive Orientation of Armed Forces	
Operational	• Limits on Maneuvers and Exercises	
Declaratory	• No first Use	
Verification	• Air- or space-based sensors	

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

Confidence and security building measures in cyberspace

IFSH
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

- Established measures vs. cyberspace
- IT and cyberspace
  - Immaterial
  - Virtual
  - Easy to duplicate
  - No specific technical facilities necessary
  - Strong dual use character
  - Difficulties with attribution

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

- "Fuzziness" of cyber attacks
  - Crime, espionage, sabotage, military attacks use (basically) the same tools
  - The effect is primary a question of the actors intention

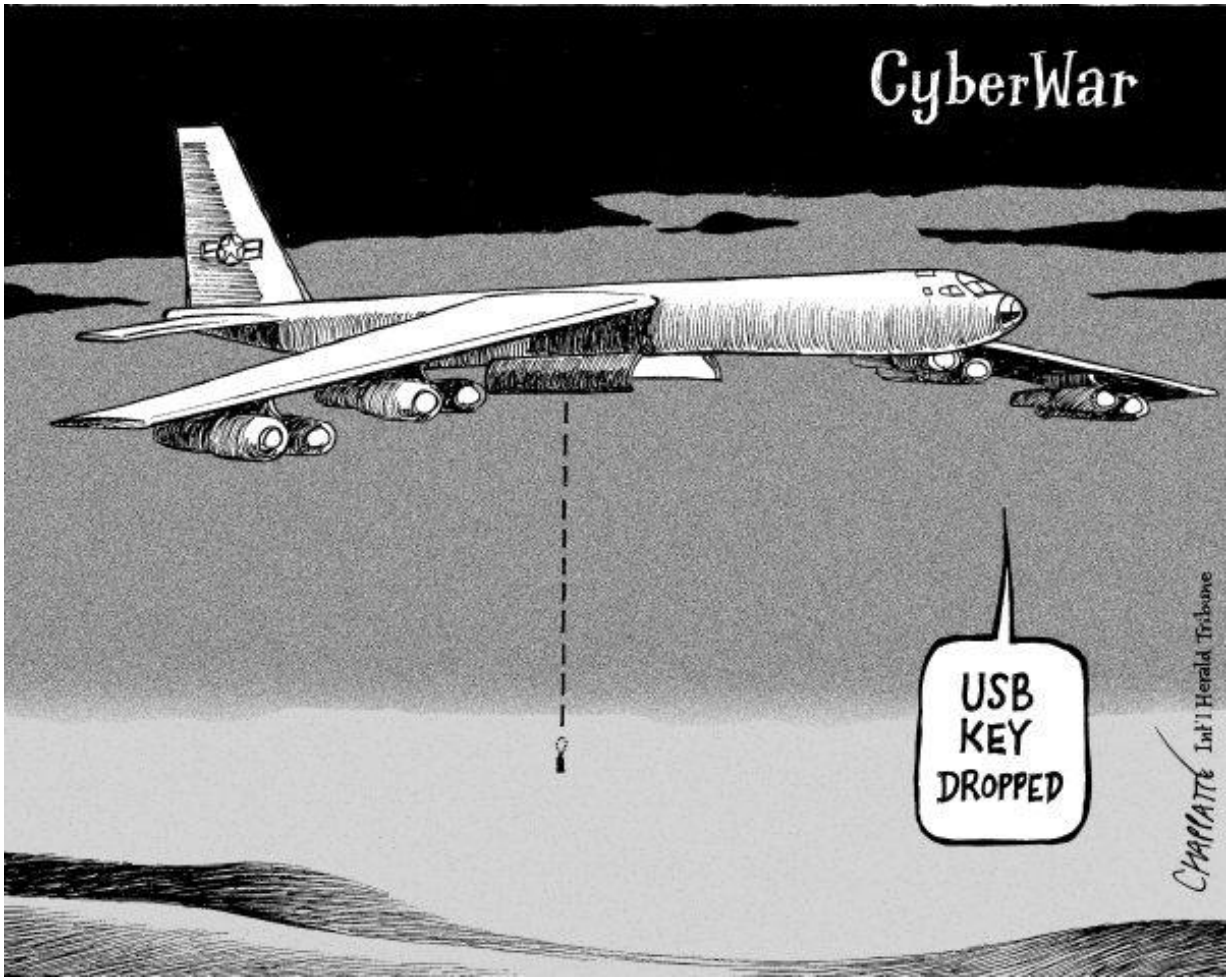
*Neuneck, G, "Confidence Building Measures - Application to the Cyber Domain", Lecture, 2012

Consequences, tasks and challenges

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Vulnerability of important systems / critical infrastructures
  - Broad evaluation of IT systems, flaws and security concepts
  - Re-Think security concepts given the reality of "omnipotent attackers"
- Effects and damages of malware are the key for their regulation
  - How to measure and classify the possible impacts of a malware?
- Better defence, but avoid concerns about better offence
  - Development for rules of engagement
  - Codes of conduct
- Cyberspace as man made domain
  - How can we create a cyberspace that support its peaceful development?
  - Technical support for trust building as well as arms control

Thanks



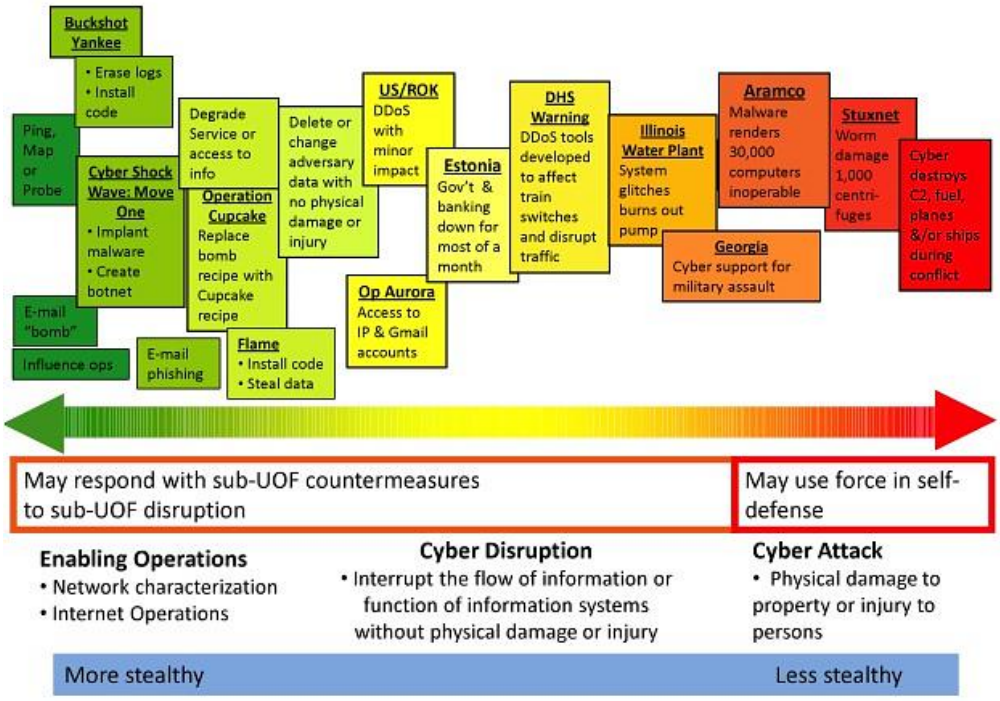
Thomas Reinhold
reinhold@ifsh.de
cyber-peace.org

Annex

On cyber weapons and cyber attacks

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 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?
  - "cyber attack" is the equivalent of "armed attack" in terms of humanitarian law
  - Position of the NATO CCDCODE Tallinn Manual



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

On cyber weapons and cyber attacks II

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- 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)

- Binding 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
  - Classification for disarmament agreements, arms control and verification
  - To confine between defence and offence

Threats, damages and the fuzziness of prediction

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Its easy to vandalise random targets but hard 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