Cyberwar on the Horizon

Stefan Schumacher

www.kaishakunin.com

DeepSec InDepth Security Conference
Vienna / Austria, 2010-11-25

解釈人

About me

- Security Consultant (`www.Kaishakunin.com`) with focus on Social Engineering, Security Awareness, Counter Intelligence and Security Management
- President of the Magdeburg Institute of Security Research and editor of the Journal
- President of the Magdeburg Academic Society of Security Policy Studies

解釈人

Table of Contents

解釈人

Table of Contents

解釈人

Introduction

Cyberwar currently is a big hype in

- the media
- IT-Security scene
- military
- politics
- political science

Think of Stuxnet, Georgia, Estonia, South Korea ...
But: Is it really possible to wage a *war* in cyberspace?

theoretical political/military science discussion

解釈人

Cyber War
Cyber

- Cyberspace: technical and social dimension
- technical: a lot of Hardware with some Software
- social: a space where people communicate and live together (Communities like 2nd Life, Facebook, Usenet ...)

解釈人

Cyber War
War

Definition (Wikipedia)

organized violent conflict of extreme aggression between at least two groups, with mortality

解釈人

War
Carl von Clausewitz

- Carl von Clausewitz, born near Magdeburg in 1780
- joined Prussian Army in 1792
- joined Prussian Military Academy in Berlin in 1801
- was aide to Scharnhorst in the reorganisation of Prussian army in 1806
- became General and Director of the Prussian Military Academy
- died of Cholera in 1831
- »On War« published in 1832 by his widow
- dialectical theoretical discussion of war
- with a focus on strategy, tactics and fog of war
- *THE* book on war

解釈人

Cyber War
War

Definition (Carl von Clausewitz)

War is nothing but a duel on an extensive scale. [...]
War therefore is an act of violence intended to compel our opponent to fulfil our will.

- War is a mere continuation of policy by other means, it has no purpose by itself
- objectives of war: to either achieve limited aims or to disarm an opponent and render him politically helpless or military impotent

解釈人

Strategy and Tactics

- tactics is the theory of the use of military forces in combat
- strategy is the theory of the use of combats for the object of the war
- winning single battles is tactics
- winning a war is strategy
- occupying a country and building a new nation is strategy

解釈人

Strategic View

- Cyberwar is a mere continuation of policy by other means, it has no purpose by itself
- Cyberwar must be embedded into a political strategy to render an opponent military impotent
- just doing some hacking can be considered as skirmishing, but not as a strategy or even a war
- IMO: Cyberwar currently is a part of conventional warfare on tactical level

解釈人

Cyberwar and military strategy

- Cyberwar might change one fundamental Clausewitzian paradigm
- *it is easier to defend than to attack*
- logistics, knowledge of area, fog of war
- Cyberwar: the defender has to defend all systems and find/patch all vulnerabilites
- the attackers only have to find one vulnerability
- a 14-year old pakistani scriptkiddie might be able to shutdown the US Air Force and start a Cyberwar
- this will have *important* political implications

解釈人

Table of Contents

解釈人

public international law

- there is no international treaty available that establishes a legal definition for an act of cyber aggression
- Law of Armed Conflict (aka International Humanitarian Law) applies
- jus ad bellum: justice to war: how to proceed to to a state of war
- jus ad bello: justice in war: how to conduct a war
- different interpretations of current LoAC exist
- generally accepted interpretations say that cyber attacks are not an act of war
- to be an act of war cyber attacks have to be conducted by governmental organizations or at least have to be supported by them

解釈人

Nonproliferation

- nonproliferation of cyber weapons is in discussion
- nonproliferation treatys are required to enforce nonproliferation on an international level
- see: nuclear nonproliferation treaty
- but: it is also a technical problem
- How shall nonproliferation be enforced? The Internet can not really be censored and cyberweapons can be smuggled on SD Disks

解釈人

NATO

- USA want to change NATO treaty to allow »conventional« military reactions to cyber attacks
- a 14-year old pakistani scriptkiddie might be able to shutdown the US Air Force
- pretending to be chinese
- and provocing a conventional attack of china
- by all NATO members

解釈人

Cyberwar ./. Cybercrime

- legal definitions of cyberwar and cybercrime have to be made
- an international cybercrime convention is required
- an international anti cybercrime agency too
- IMO cybercrime is currently more dangerous than cyberwar

解釈人

Table of Contents

解釈人

Stuxnet
A strategic view

- Stuxnet was expensive, several good programmers + management
- testbed including industrial computers and controll devices
- well organized group (military?)
- used multiple 0day exploits (expensive to find or buy)
- used multiple intrusion vectors, including USB sticks in very sensitive areas like nuclear research plants
- a well organized, strategically planned act of aggression
- but did it disarm an opponent and render him politically helpless or military impotent?

解釈人

Stuxnet
A strategic view

- Stuxnet was expensive, several good programmers + management
- testbed including industrial computers and controll devices
- well organized group (military?)
- used multiple 0day exploits (expensive to find or buy)
- used multiple intrusion vectors, including USB sticks in very sensitive areas like nuclear research plants
- a well organized, strategically planned act of aggression
- but did it disarm an opponent and render him politically helpless or military impotent?

解釈人

Smartmeters
a new attack vector

- EC wants »intelligent« electricity meters in all households
- remotemeters measure the detailed amount of power consumption
- intention: to help save electric load and gahter information for powerplants
- industry and powerplants are interested in so called smartmeters
- smartmeter allow powerplants to remotely shutdown a household

解釈人

Smartmeters
a new attack vector

- if a lot of households are shutdown at the same time, the cut off current might shutdown the local power plant
- the shutdown of the local power plant produces more cut off current
- which can create a cascading effect to the next power plants
- almost all european power plants are cascaded into one network
- backup systems rely on natural gas
- North Italy was shutdown by an accident and a cascading effect

解釈人

Smartmeters
a new attack vector

- if a lot of households are shutdown at the same time, the cut off current might shutdown the local power plant
- the shutdown of the local power plant produces more cut off current
- which can create a cascading effect to the next power plants
- almost all european power plants are cascaded into one network
- backup systems rely on natural gas
- North Italy was shutdown by an accident and a cascading effect

解釈人

Smartmeters

- currently, there is absolutely no IT security involved in the process
- a lot of power companys and industrial companys can make a lot of money
- they are lobbying for the introduction of smart meters
- smart meters are bloated like Emacs to make them expensive
- that process needs to be analyzed by political science

解釈人

Outlook

- Network Centric Warfare (»data warehousing«) central doctrine of US armed forces
- heavily relies on electronic communication – which can be hacked to render military units unable to act
- robotic warfare/surveillance drones (»Terminator«) heavily rely on electronic communication
- perspective trojans?

解釈人

Coda

- the term cyber*war* is IMO exaggerated
- it is currently not possible to render an opponent military impotent
- but we are working towards a society that relies more and more on IT
- an we have absolutely no international strategy on IT security
- we are currently in an experimental phase (Airforce; Panzer)
- read Clausewitz, Weizenbaum and van Crefeld

解釈人

Night Talk on *Security Awareness*

Any Questions?

Stefan.Schumacher@Kaishakunin.com

解釈人