Assessing the Hacking Capabilities of Institutional and Non-institutional Players

Stefan Schumacher

www.sicherheitsforschung-magdeburg.de
Magdeburger Institut für Sicherheitsforschung

DeepSec 2016



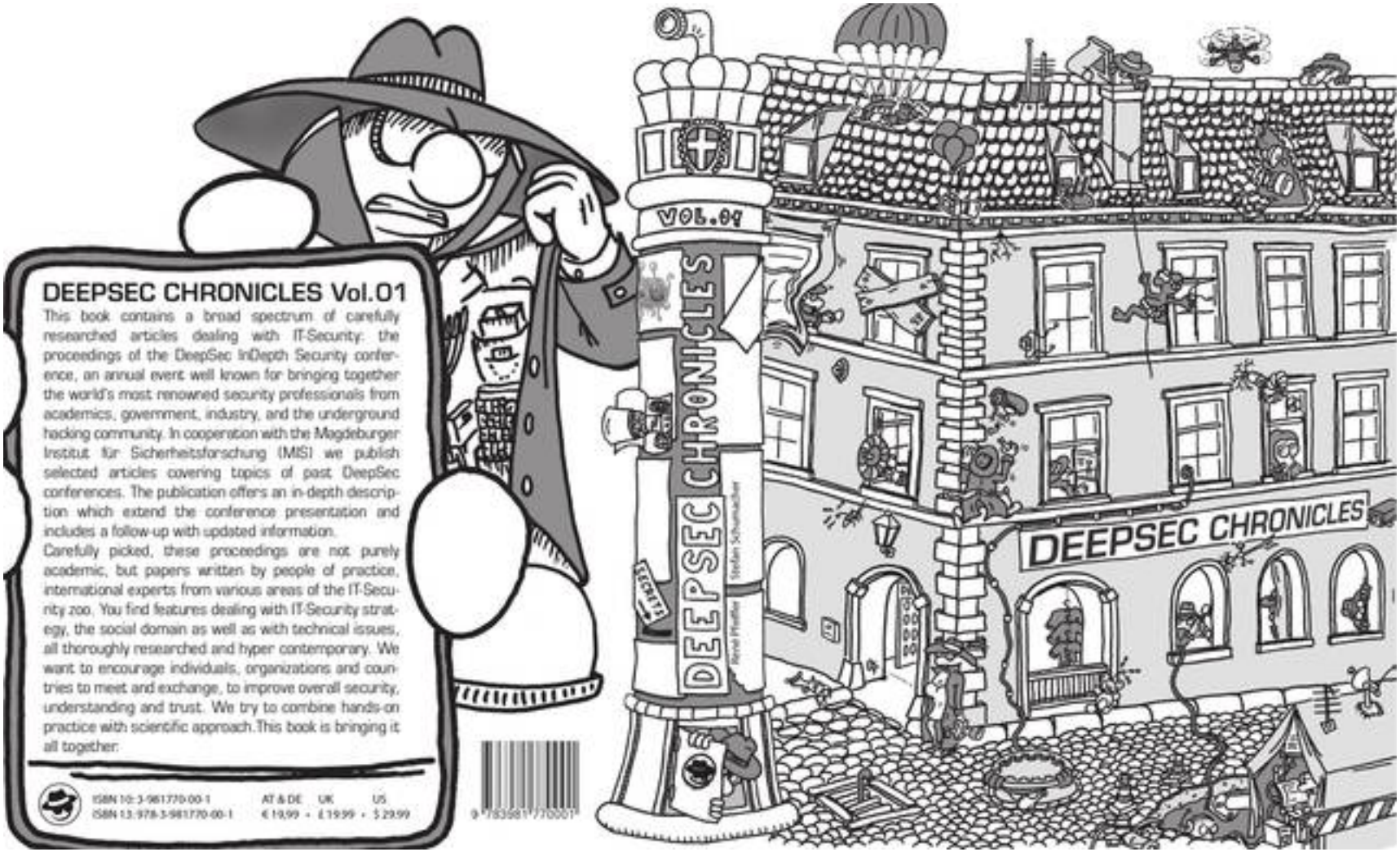
Über Mich



About Me

- Hacker for 20+ years, ex-NetBSD developer
- Educational Science and Psychology,security researcher
- Psychology of Security
- Social Engineering / Security Awareness
- Psychological Profiling for Social Engineering Attacks
- Evaluation of Security Awareness Campaigns
- Didactics of Security/Cryptography
- Construction of Security in Individuals (qualitative research)
- Trainings for German law enforcement and armed forces
- publications on Cyber Cyber (war, terror etc.)



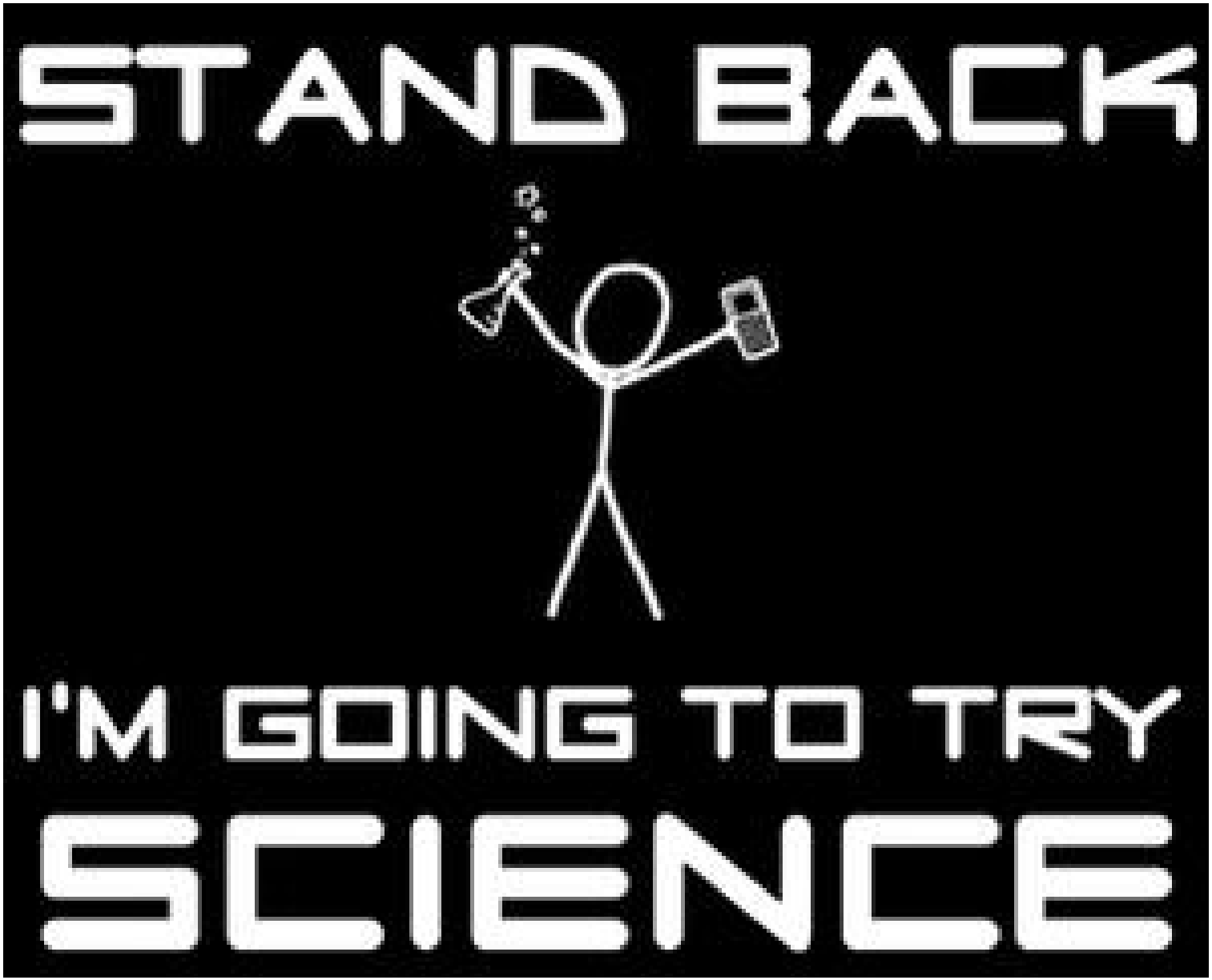

DEEPSEC CHRONICLES Vol.01
This book contains a broad spectrum of carefully researched articles dealing with IT-Security: the proceedings of the DeepSec InDepth Security conference, an annual event well known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. In cooperation with the Magdeburger Institut für Sicherheitsforschung (MIS) we publish selected articles covering topics of past DeepSec conferences. The publication offers an in-depth description which extend the conference presentation and includes a follow-up with updated information.
Carefully picked, these proceedings are not purely academic, but papers written by people of practice, international experts from various areas of the IT-Security zoo. You find features dealing with IT-Security strategy, the social domain as well as with technical issues, all thoroughly researched and hyper contemporary. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security, understanding and trust. We try to combine hands-on practice with scientific approach.This book is bringing it all together.
ISBN 10: 3-981770-00-1
ISBN 13: 978-3-981770-00-1
AT & DE
€ 19,99
UK
£ 19.99
US
$ 29.99
Vol.01
DEEPSEC CHRONICLES
Stefan Schumacher
DEEPSEC CHRONICLES

Definition (Outrage as a Svc @OaaSvc)

Science is awesome. You aren't doing science in infosec. Why not? Seems to be the overriding message of @0xKaishakunin #AusCERT2014



Stand Back!



Disclaimer

- exceptional permission A-38
- to use *cyber*
- in all forms and shapes

Cyber Cyber Cyber

- Cyberwar on the Horizon
- On Cyber-War
- Does Cyber-Terrorism exist?
- huge debate in the media and politics
- not every journalist/politician understands cyber cyber
- media hype
- FAZ: Russia is going to hack the German federal election in 2017

Excuse

- *We got hacked by state sponsored 31337 cyber war hackers ...*
- sounds better than
- *we didn't pay for a security analysis, we got infected with a crypto-trojan and forgot to make backups*

Problems

- How can we assess the hacking capabilities of actors?
- Without too much political BS
- and a sound scientific foundation
- measuring/assessing things is the core competency of Psychology
- CS/EE/natural science have a different theory of science than social sciences/humanities

Heinz von Foerster

Definition

The hard sciences are only successful because they are discussing soft problems.

Don't fall for variables that can be measured easily!

Constructs of Cyber Cyber

- Security, Hacking Capabilities, Cyber Cyber Something etc. are *constructs*

  Security is a latent social construct and has to be treated as such. Psychological and sociological methods and tools are required. If the security of a system should be enhanced, a diagnosis, prognosis and intervention is required.

Latent Social Construct

- Construct: cannot be directly measured
- can only be measured by using manifest variables to estimate the latent variables
- examples: Intelligence: Phrenology or IQ-Tests
- security cannot be measured directly
- operationalisation of security required

Cyber Cyber

- What exactly is Hacking?
- What are Cyber-Attacks?
- What is Cyber-War?
- What are the capabilities of Hackers?
- We have to make a definition and find ways to measure it
- Think of intelligence!

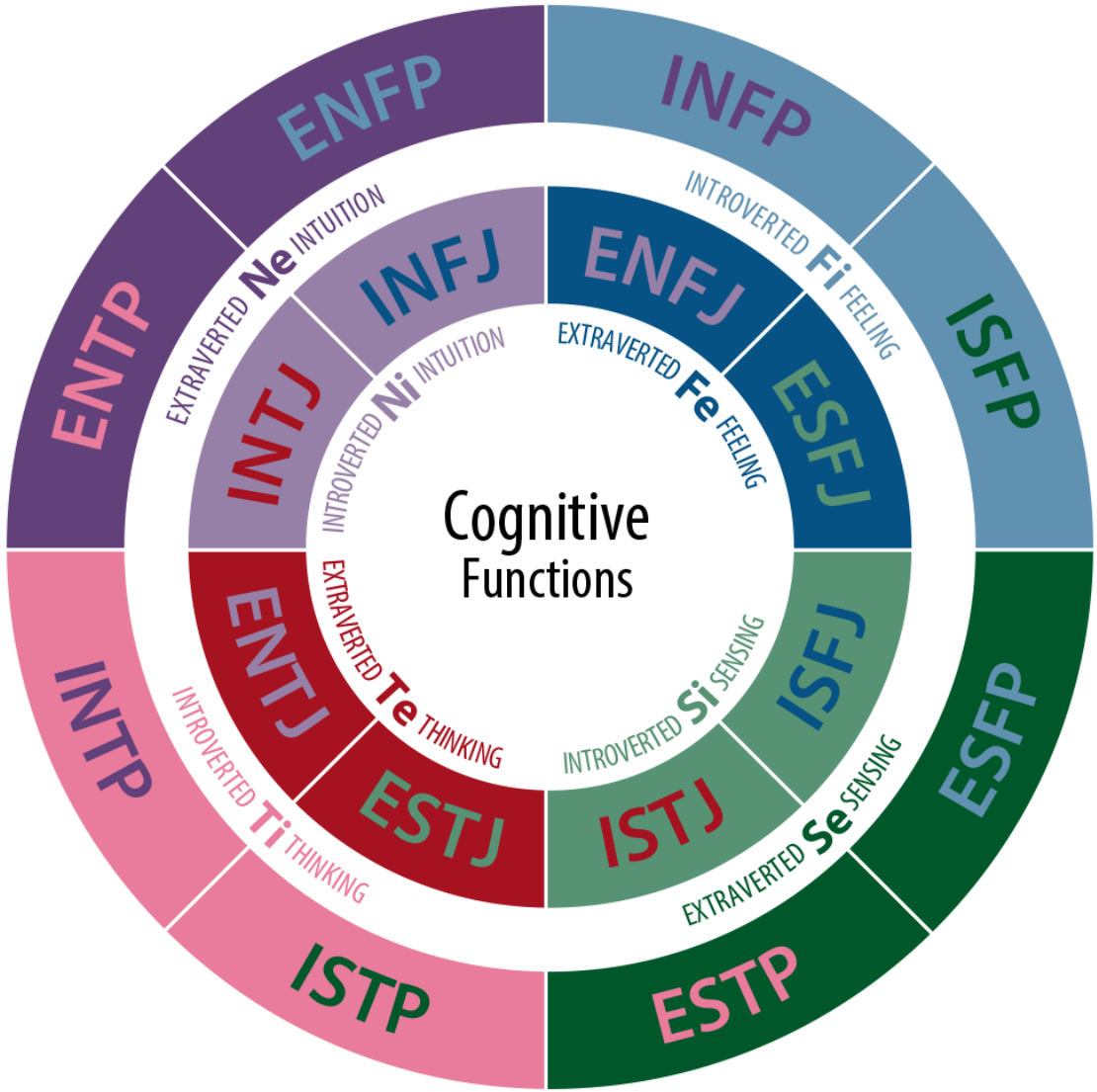
A good measurement

- **Reliability**: the overall consistency of a measure; measurement produces similar results under consistent conditions
- **Objectivity**: the standard of a research study such that its hypotheses, choices of variables analyzes, gauges made, methods of control, and observations are lacking bias as much as is possible
- **Validity**: Construct V. the magnitude to which an analysis or tool is able to gauge an abstract characteristic, capacity, or construct.

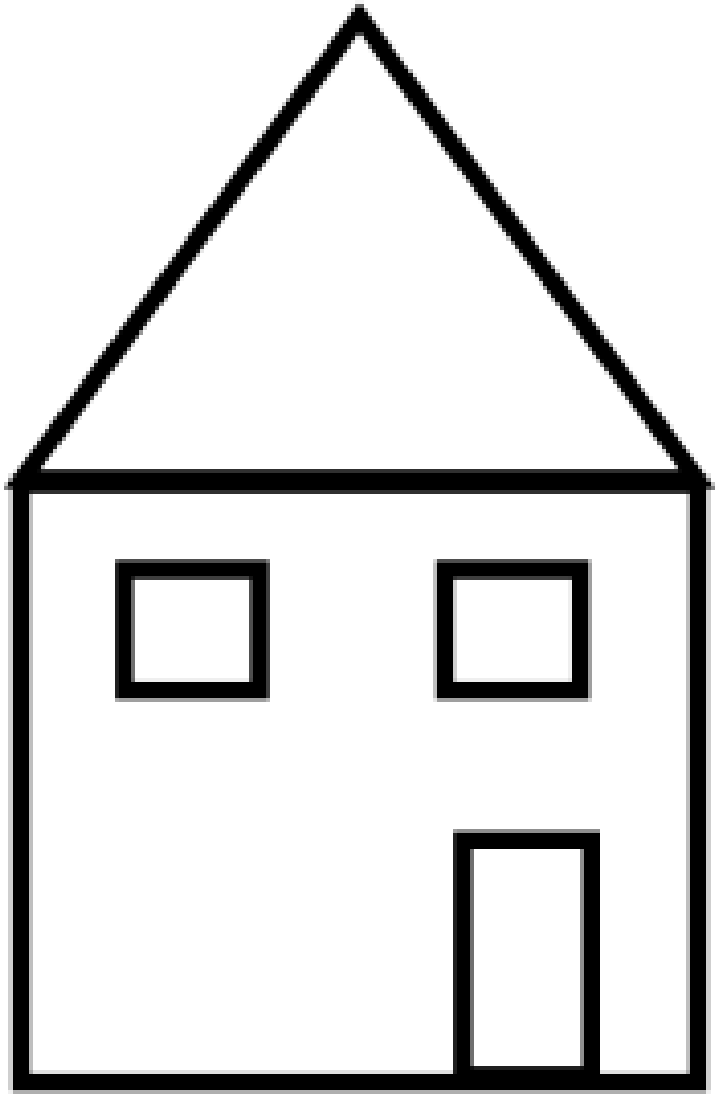
Phrenology



Myers-Briggs Type Indicator



IQ Test and Culture



How can I measure Cyberwar capabilites?

- Let's have a look at traditional military measurements

Sword vs. Shield

- Austro-Prussian-War 1866: Dreyse Needle Gun, rail network, command structure
- 1906: Dreadnought $\rightsquigarrow$ Anglo-German naval arms race: Race of Ressources! UK tried to outspend Germany $\rightsquigarrow$ lead to a heavy political crisis in Germany and birth of Social Democracy
- WW1: Range, Accuracy, Rounds per Minute of Artillery
- WW1: Chemical Weapons vs. Personal Protective Equipment : French Army in 1914
- WW2: Heinz von Guderian command structure, radios and fire on the move

Production capabilities

- Nuclear Weapons States and States that can produce NWs easily (DE, JP)
- Aircraft and Anti Aircraft
- Naval Systems
- Domestic Suppliers

Traditional Measurements

- Active Personnel, Reserve Personnel
- Budget (in % of GDP)
- Population (Number, Age, Pyramid)
- Youth Bulge (number of young men compared to number of old men)
  Afghanistan, Saudi Arabia, Africa, China vs. Europe, Japan
- Kriegsspiele (Wargames): preparation for battles
- Strong European Tank Challenge: won by Germany, followed by Denmark and Poland

Cyber War

War

Definition (Wikipedia)

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



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

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



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
- *It may sound strange, but for all who know War in this respect it is a fact beyond doubt, that much more strength of will is required to make an important decision in strategy than in tactics.*

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
- We cannot compel our opponent to fulfil our will by using cyber attacks
- IMO: Cyberwar currently is a part of conventional warfare on tactical level

Cyber War

- Cyber capabilites have to be incorporated into traditional military capabilities
- militaries use electronic warfare at least since WW1
- Prussian Optical Telegraph built in the 1840s!
- Most militaries are familiar with electronic warfare
- there is a lot of hype going on about cyber war

Hype of Cyber

- Why is there a hype of Cyber going on?
- It's cool, it's sexy
- it brings in more money and personnel, the military get's more ressources
- small actors can start to play that game, too
- setting up a tank batallion is expensive
- setting up a navy even more so

Leo 2



500 million € developmental costs for the Leopard 2
120mm training ammunition costs 1500 €

Military Paradigm

- it's easier to defend than to attack
- Fog of War, Logistics, Knowledge of Areas help the defenders
- NetBSD:ca. 163 000 files, 57 228 442 LoC, 1 991 091 842 characters
- verification practically not possible

Military Paradigm

- The victim can decide if it is attackable!
- Who forces us to put nuclear power plants online?
- What if we shut down our part of the internet?
- Or at least vulnerable systems?
- Do we have offline fall back systems?
- What if my enemy hasn't reacher the cyber age yet?
- Cyberwar against Somalia? ISIS? Al-Kaida? F.A.R.C.-E.P.?
- Estonia 2007, Georgia 2008?



Military Cyber-Paradigm

- The victim can decide if it is attackable!
- let that sink in
- The evil Russians™ cannot hack the German federal election because it is completely offline. And we have a paper trail.



What about Cyber Terrorism

- similar to Cyber War but with different goals and players
- change the government and political form of a country
- with cyber attacks

Cyber Terror Actors

- »traditional« terrorist groups
- RAF, IRA, ETA, PLO, FARC-EP, Al-Qaida ...
- Cyber terrorists
- Cyber-Djihad, Anonymous, Syrian Electronic Army
- Where do they come from?

Growing Cyber Terrorists

- Background, Culture, Educational System
- Do Hacking groups exist in their countries?
- Chaos Computer Club Riyadh?
- Hacking is **not** formal training!
- Having a MSc, PhD, MCSE, NCNE ... does not make you a hacker
- Weltanschauung!



Growing Cyber Terrorists

- terrorist groups can send their members to study CS, EE, Maths
- send them into hacking groups
- can you imagine a hardcore salafist joining a Hacker space?
- they might turn into a hacker, but then they are no longer salafists
- or they will stay salafists, but then they won't become hackers
- Hacking operations by terrorists currently limited to rather simple attacks
- guessing the primitive password of a Twitter account is not cyber war
- or the end of the world as we know it



Honeypots

- we could set up honeypots or a whole honeynet
- to identify and measure attacks
- and their complexity
- consequence for the attacker: Did they attack a real system or a honeypot?
- Is the stolen data correct or manipulated?
- second independent source required!



Social Engineering

- How do you want to detect a distributed SE attack?
- How do you want to prevent something we don't know if it is happening?
- strategic communication/PsyOps is an old field of military work
- hydrid conflicts as in the Ukraine might be the new standard conflict

Résumé

- measuring the cyber capabilites as a multidimensional variable
- in a reliable, objective and valid way
- combine those dimensions
- eg. economic, financial, educational benchmarks, youth bulge, industrial capabilities
- analyse openly known political/tactical doctrines

Résumé

- to much cyber cyber is going on
- to much technobabble by people who don't understand hacking/IT
- relax and don't panic
- do more science!

- Psychology of Security - A Research Programme, Stefan Schumacher
  `http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_041_SchumacherPsychology.pdf`
- Die psychologischen Grundlagen des Social Engineerings, Stefan Schumacher
  `http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS-001.pdf`
- Vom Cyber-Kriege. Gibt es einen Krieg im Internet? by Stefan Schumacher
  `http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS-018.pdf`

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co