Einfuehrung in die Cybersicherheitspolitik

64553 characters in 7966 words on 1584 lines

Florian Moser

December 15, 2020

1 einführung

wechselwirkungen staat/gesellschaft/wirtschaft
wirtschaftlicher wandel; bedrohungslage, bedrohungswahrnehmung
gesellschaftliche entwicklung; sicherheitstrategien / -praktiken
staat koordiniert, technologie ermöglicht

cyber
beziehung zu digitalem raum ("cyberraum")
virtueller datenaustausch über kabel/protokolle im cyberspace
je nach akteur wird cyberspace anders verstanden / definiert
vulnerability-multiplier (risiko für cyberspace)
force-multiplier (risiko durch cyberspace)

sicherheit
ein "essentially contested concept"
somit exakte definition nicht möglich
da empirische beweise, sprachgebrauch, logik nicht ausreichend
versuch der definition führt lediglich zu endlosen debatten
"absence of threat to acquired values" (wolfers)
"war made the state, and the state made war" (tilly)
für wen/was, vor was, wie umgesetzt (preis, mittel, perfektionismus)

politik
entscheidungen von und für gruppen von menschen
"muster menschlicher beziehungen mit macht/herrschaft/autorität"
besteht aus polity (strukturen), politics (prozesse) und policy (inhalte)
gesellschaft als drei sektoren (regierung, privatsektor, zivilgesellschaft)

cybersicherheit
maintains / creates a collection of tools, policies, organisation
to protect cyber environment & assets (information, tools)
general objectives are availability, integrity and confidentiality
integrity may includes authenticity and non-repudiation
sicherheit die nation im und vom cyberspace geniesst

sicherheitspolitk
"hochpolitik" (da sicherheit von grundlegender bedeutung)
früher "bedrohung, einsatz und kontrolle militärischer gewalt"
jetzt ausweitung auf "terrorismus, pandemien, klimapolitik, ..."
verwundbarkeit der gesellschaft als thematik
prävention von sicherheitsvorfällen wird wichtiger
daher zunehmend überwachung, risikomanagement

cybersicherheitspolitik
digitale technoligien (insb. gebrauch durch menschliche akteure)
aushandlungsprozesse (festlegung verantwortlichkeit, gesetze, ...)
cyber-sicherheitspolitik (sicherheitspolitische aspekte)
cybersicherheits-politik (cybersicherheit im allgemeinen)

2 trends in cybersicherheit

2.1 cyber-risiken

diverse phänomene (krieg/terror, sabotage/spionage, kriminalität, hacktivismus)
diverse schäden (politische, physische, reputation, ökonomisch)
makro risiken für kritische infrastrukturen
mikro risiken für daten / wissen
oft schwierige attribution

2.2 strategisch

opportunität, können und nutzen alles vorhanden
marktbedingtes sicherheitsdefizit (mehr geräte & daten, kritischere nutzungen)
professionalisierung im crime bereich (markt für sicherheitslücken)
politisch-strategischer nutzen (protest, spionage, störungen, manipulation)

2.3 geschichte

von operationellem cyberkrieg
wie 1998 kosovo konflikt; nutzung InfOps als teil konflikt?
zu störaktionen
wie 2007 ddos attacke estland; nato verteidigungsfall?
wie 2008 anonymous; hacktivismus
zu staatlicher spionage
wie 2010 stuxnet; fähigkeiten staaten & regeln?
wie 2013 snowden; fähigkeiten geheimdienste?
wie 2014 sony hack; klare attribution der US regierung
zu strategischer manipulation
wie 2016 US wahlen; strategische täuschung
nun ernsthafte sicherheitsthematik (national/international)

2.4 cyber-macht

hacktivismus, cyber-kriminalität, strategische nutzung
professionalisierung von cyber-söldern
steigende preise bei schwachstellen
patriotische hackergruppen ("plausible deniability")
cybermittel werden in aktiven konflikten getestet
hotspots sind USA vs Russland/China, Ukraine, Syrien, Europawahlen
spear fishing (personalisiertes fishing), malware, DDoS
betroffen sind staat oder strategische akteure wie medien
angemessene reaktion schwierig (attribution, verhältnismässigkeit)

2.5 cyber-konflikt

nutzung cybermittel spezifisch zu konflikt
hacktivismus als bürgerprotest (bürgerkriege, repression)
information warfare / sabotage (hybride kriegsführung)
rekrutierung, finanzierung (terrorismus)
organisation von streitkräften (operationeller cyberkrieg)
nachrichtendienst & informationskriegsführung rückt im vordergrund
noch zurückhaltender gebrauch, da wirksamkeit nicht abschätzbar
weniger black-ops, mehr kontinuierlicher einsatz

2.6 schutzstrategien

seit 1998 IT security / information assurance
seit seit 2007 resilienz / risikomanagement
seit 2010 cyber als nationale sicherheit / grand strategy
eskalationsgefahr bannen, system stabilisieren

zur abschreckung/verteidigung
aufbau staatliche fähigkeiten (beschaffung/nutzung technologien)
militärdoktrin (cyberoperationen integrieren)
politischer zielkonflikt (geheimhaltung vs abschreckung)

für cyber-normen
kriegsvölkerrecht (definition cyber waffe)
China-USA abkommen (wie strategische stabilität aufrecht erhalten)
public-private partnerships (wie soll staat diese nutzen)
internet gouvernanz (wer soll regieren)

2.7 cyber-security als gemeinsame verantwortung

gegenmassnahmen
technische (IT security)
organisatorische (crisis management)
gesellschaftliche (sensibilisierung, ausbildung)
politische (schutz kritischer infrastrukturen)
rechtliche (gesetze, regulationen)

akteure
staat (bund/kantone)
wirtschaft (grossfirmen, KMU)
gesellschaft (generationenabhängige bedürfnisse)

3 geschichte der cybersicherheitspolitik

sicherheitspoltik über überlebensfragen kollektiv (staat, wirtschaft, gesellschaft)
grundfrage der relevanz von informationssicherheit zur sicherheitspolitik

3.1 sicherheitspolitische konzepte

technologische treiber
entwicklung/nutzung digitaler technologien
wie prägung durch/von politische ideen / machtstrukturen
wichtige ereignisse inner- / ausserhalb des cyber bereichs

politische treiber
internationale (macht) politik
wie die entstehung neuer machtquellen/cooperationen
innenpolitik (verhandlungen über rollen/verantwortlichkeiten)

marktwirschaft
(hier nicht näher beschrieben, aber auch einflussreich)

3.2 treiber der entwicklung

inhalte (policy) und praktiken (politics) anderer staaten
mobilisierung eigener ressourcen die ansichten prägen
nicht-staatliche akteure die cyberspace (miss-)brauchen
fokussierende ereignisse (cyber vorfälle)

3.3 empirische entwicklung

3.3.1 80er

spionage von regierungscomputern (nationale sicherheit)
noch kein massenphänomen (technische limitierungen)

diskurs
virus & würmer entstehen → technische unsicherheit
computerkriminalität → rechtliche unsicherheit
populärkultur wie "war games" → "was wäre wenn" szenarien
spionage wie "cuckoo's egg" → frage der zuständigkeiten
policy-communit reagiert auf hacking als "gefahr"

3.3.2 90er

bedrohung durch terrorismus, rogue staates
abhängigkeit von vernetzten systemen & kritischen infrastrukturen

diskurs
91 golfkrieg als erster informationskrieg
pentagon vermehrt ziel von angriffen (94, 98, 98)
96 RAND exercise, 97 elligible receiver exercise
übungen & daraus gezogene lehren wichtig für polcy building

breiterer sicherheitspolitischer kontext
blick auf asymmetrische bedrohungen / nichtstaatliche akteure
einschätzung schwierig wer gegner ist / welche capabilities
blick daher auf verfügbare gefährliche tools
sowie eigene verwundbarkeiten

kritische infrastrukturen
critical foundation report 97 verbindet cyber mit infrastruktur
vorfälle, übungen, studien zeigen reale gefahr & problem
neue verwundbarkeiten durch softwaresteuerung
neue möglichkeiten attacker (günstig, schnell, anonym)
liberalisierung der kritischen infrastrukturen (zT in privater hand)

3.3.3 00er

qualität/quantität cybervorfälle steigt, staaten werden involviert
neuer fokus auf information operations
nutzung geheimdienste mit plausible deniability

diskurs
post 9/11 umstrukturierung verantwortlichkeiten / strukturen
fokus von cyber security wird in frage gestellt
Al-Qaida + cyber nachforschungen (welche capabilities)
operationeller cyberkrieg (zunehmende verwendung von cyber tools)
wenig offensiv (hacken anderer), eher unterstützung
organisierte kriminalität (markt organisiert sich, seltener einzeltäter)

dynamiken
diskussion zu wie gefährlich, was ist gefährlich
staaten rüsten auf (zuständigkeiten, zusammenarbeit mit privatsektor)
fokus auf rogue states (wie wahrscheinlich ist cyber terror)

3.3.4 10er

steigende qualität, quantität, öffentliche aufmerksamkeit
staaten rücken immer mehr im hintergrund; defensiv & offensiv
durch staatlicher fokus nun auch cyber-"wettrüsten" relevant

events
wikileaks, anonymous (hacktivismus, fokus auf geheimhaltung)
festnahmen nach attackierung high-level ziele
darum heutzutage weniger hacktivismus
stuxnet (fokus auf cyberkrieg & staatliche fähigkeiten)
snowden (fokus auf cyberspionage)
US election hacks (fokus auf information operations)

stuxnet (juli 2010)
computerwurm, sehr komplex & aufwendig in der entwicklung
kein diebstahl, botnet; aber sabotage von industrieanlagen
hoher befall im iran & verzögerung atomprogramm
fazit strategisch eingesetzte cyberwaffe
gefunden durch verursachte bluescreens
2012 in times "bewiesen" durch whistleblower
möglicherweise zur verhinderung eskalation konflikt durch israel

trollfabriken (seit 2008).
kontinuierliche beeinflussung von diskussionen in öffentlichen foren
jedoch unklar ob beeinflussung strategisch relevant ist
wie ukraine konflikt beeinflussung

hacking/schmierkampagnen (seit 2016)
während wahlen zur destabilisierung politischer prozesse
frage wer interesse an destabilierung hat
wie wahl USA (effektiv); wahl EU (weniger effektiv)
wie fake news die vertrauen medien untergräbt

medien
viel aufmerksamkeit in den medien, inklusive stuxnet

advanced persistent threat (ATP)
mehrjährige cyberoperationen
nur staaten genügend mittel / interesse diese durchzuführen

3.4 rollen des staates / problemfelder

schwierige garantierung sicherheit für nicht-staatliche infrastrukturen
attackers werden mächtiger, defense wird schwieriger
schutzaufgabe staat schwieriger (PPP, uneinigkeit innerhalb staat)

cybersicherheit inland
höheres sicherheitslevel stabilisiert ökonomie / kritische infrastrukturen
in liberalem staat lieber kooperation als zwang
mit PPP auch eigene machtlosigkeit eingestanden

cybersicherheit ausland
staaten suchen nach kooperationspartner
möchten jedoch auch eigene macht ausbauen
sicherheitdilemma (eigener raum sichern, andere bleiben attackierbar)

dilemma nicht-staatlicher infrastrukturen
staat möchte für schutz der bevölkerung sorgen
aber netzwerke nicht in staatlicher hand
gesetzesänderungen oder riesige ausgaben unrealistisch
daher kooperation mit PPP für definition & umsetzung nötig

bürokratische machtpolitik
verschiedene legitime perspektiven
wie IT sicherheit, ökonomie, strafverfolgung und nationale sicherheit
priorisierung, verantwortung, ressourcen, schulungen unklar
konzepte/policies alle paar jahre neu verfasst

rollen (intern)
schützt eigene systeme & bevölkerung
privatsektor schützt eigene systeme, insb. kritische infrastrukturen
gesellschaft schützt eigene geräte (bürgerpflicht)

rollen (extern)
staaten anarchisch untereinander
"anything goes" mit geheimdiensten solange nicht attribuierbar
jedoch auch kollaboration, austausch untereinander, entwicklung policies
privatsektor möchten normen
gesellschaft als beobachter/einflussnehmer (konsultation, hacktivismus)

3.5 (source) cybersecurity pre history

by michael warner, 2012

introduction
technological advancement motivates new vulnerabilities
argues headlines about hacks & cyber war are not new
since 1960 computer have sensitive data & need protection
since 1970 computer can be attacked & data stolen

since 1980 computer can be used by the military
since 1990 others might apply this technique

sensitive data & need of protection
1967 any multi-user system poses threat to its data
by software, hardware, human actors
1970 hashed passwords, administrator privileges, file system permissions
1978 DES introduced by NSA (encrypted communication)

attacking of computers
1980 global networks introduced + virus & hacking became popular
military programs insecure (like technicians with admin access)
CIA wanted to share data to other agencies relative to security level
but project aborted due to root access in penetration test
1979 data integrity issues arose leading to failing systems
1983 highschool students penetrated military networks
1984 NSA in charge for standards, guidance, monitoring, research
of all government telecom systems & automated information systems
but in debate uncertainty about such high impact of military agency
1987 NSA secures national security networks (.giv, .mil), NBS others

military use of computers
1970s with vietnam war started to use digital sensors on battlefield
1980 modified devices shipped to UDSSR to sabotage / spy
1991 swift war in kuwait, first "information war"
1993 military policy to disrupt command and control systems
prevent info flow, sabotage (deceipt & kill), introduce doubts
1993-4 Air Force, Navy and Army introduced Information Warfare centers
1996 replaced term by information operations, but intention got out
serious doubts using american computers & software in other govs
other countries build up capabilities, recognising missing attribution

others have the same capabilities
1985 denial of service attacks recognised by NSA
1991 increasing risk of hackers to own data recognised
1988 morris worm, 1992 michealangelo virus, 1996 DoS of ISP in new york
1995 security exercise revealed large flaws in US system
1996 attacks to military networks happened, DoS attacks common
recognised not enough spending in security opened up new vulnerabilities
attribution is hard, execution cheap, legal prosecution difficult
"telefon connection anywhere in the world enough to cause harm"
1997 exercise shown US is open to digital attacks by low-staffed team
2001 intrusion into power system unnoticed for weeks

3.6 (source) cyber security

by myriam dunn cavelty

information security 101
cyberspace & internet almost used interchangeably
cyber-security for both security in and from cyberspace
internet evolution of ARPANET, without security in mind
IT security no return in investment, slow, expensive, bad usability
big data / advertising as additional incentives for unencrypted data
security services such as NSA work to make it less secure
hacker ethics as sharing, openness, free access to information
malware to steal, disrupt, corrupt data (such as worms, trojan horses)
social engineering as way to grab passwords / gain access

cyber-security story
originated in the US in 70s, spread to the world in the 90s
constantly changing as technical landscape develops
70s, 80s about securing systems
90s about reliable operation of critical systems
2016 about strategic manipulation as threat to democracy
technical discourse (by computer experts against malware)
cyber-crime/espionage discourse (by law enforcement for business)
cyber-war / infrastructure protection discourse (by military for forces)

virus history
1988 morris which made ARPANET unusable
1992 michelangelo which overwrote harddisks with 0s
1998 back orifice as trojan horse
1999 melissa which shut down emails
2000 i love you which propagated over email
2001 code red which defaced websites / DDoS
2001 nimba as trojan horse
2003 blaster / slammer DDoS
2007 zeus stole banking secrets, botnet
2008 conficker which formed botnets
2010 stuxnet which sabotaged industrial systems
2011 duqu as copy-cat of stuxnet by US
2012 flame used for espionage by US
2014 regin for espionage by US
2013 WannaCry as randsomware
from easy mass-target worms to sophisticated targeted tools
from hobbiists to criminal / strategic usage
attribution problem makes prosecution hard

cyber incidents
1982, 1986, 1994 break-ins into USA high-profile systems
1994 bank robbed online
1998 computer networks attacked, networks probed for attack vectors
2003 access to high-profile system in the US
2007 zeus botnet controlled millions of machines
2009 GhostNet infiltrated political, economic, media locations
2009 Aurora tried to modify code at google et al
2010 wikileaks leaks diplomatic cables
2010 operation avenge assange attacks anti-wikileaks behaviour
2011 CO_2 emission papers stolen
2013 NSA leaks shows extent of NSA operations
2014 sony pictures hack which delayed The Interview release
2015 personal data of applicants for US government stolen
2016 US election hack with stolen sensitive data about election candidate

trends
cyber groups well organized, from fraud to money laundering
western state start to use cyber espionage (used to be china)
hacktivism to publish infos, destabilize or humiliate

cybered conflict
after 1991 gulf war US military recognised information as weapon
first only at military systems, extended to other systems
like media disinformation, DDoS attacks, rumours, webpage defacements

cyber conflicts
1991 gulf war used information warfare by US
1999 operation allied force as internet war by US
2000 cyber-antifada by palestinian
2001 cyber world-war 1 by hacktivists to US & China
after US surveillance plane forced to land on china soil
2007 estonia DDoS by russian government, NATO question
2008 georgia DDoS by russia government
2010 stuxnet by US & israel
2011 korean network intrusion by north korea
2011 syrian conflict involvements by hacktivists
2013 ukraine conflict involvements by russia
stuxnet as wake-up call for armies, policies

reducing cyber-insecurity
protect crucial networks by special infrastructure protection
(done by other agency than those using network)
use public private partnerships (PPP)
information assurance, risk management following CIA
increase resilience (recover from shock) bc can not fully prevent incidents
technically reduce with certification & standards
espionage reduce with law (including international regulations)
military reduce with arming (+international behaviour norms)

recent developments
2013 consensus that humanitarian law applies in cyber space
no willingness to forgoe offence use of cyber weapons
difficult to verify / control capabilities of states
many technologies have dual use purposes
trends look like political solutions at policy level

about relevance
cyber-incidents have caused so far only minor outages
but more and more states invest in weapons
cyber-fears grow and motivate military controlled solutions

conclusion
investing in cyber weapons potentially very expensive
solving attribution problem would kill privacy
research has little data besides DDoS attacks
need to find response to security threats in real contexts

3.7 (source) zero days

movie 2016

3.7.1 cyber warfare

kind of attackers
traditional hackers for money
hacktivists for fun / political
nation states for high quality intelligence or sabotage

new capabilities
high speed attacks & low attribution possibility

supply troops with newest intel about proximity

the need for policy
need governance on how weapons may be used
at the moment "do whatever you can get away with"

comparison to nuclear weapons
in cold war many nuclear weapons created
but no clear strategy existed on how to use it
after 20 years of public debates, including in russia
treaty signed to clear up things

intransparency
states do not talk about offence (only defence)
for policy, need public debate & many years of dialogue
but capabilities not talked about
uncertainities on how to enforce (how to inspect computers?)
forces in power do not want to start it

3.7.2 iran atom bomb conflict

iran vs israel and allies
iran repeatedly declared it wants to destroy israel
2010 nuclear scientists murdered in iran

nuclear history of iran
allied to USA when gouverned by shah
given the first nuclear reactor
1979 islamic revolution
blocks of trade by US (including nuclear)
knowledge from packistan (started 95 with own atomic bomb)
2001 invasion of irak
then iran wanted to pursue atomic bomb more seriously
2008 started to get serious
2010 stuxnet & assassination of key personnel
2014 abkommen

israel/us responses
1981 israel bombs irak nuclear reactor in bagdad
2006 israel wants to bomb iran, but US refuses
likely israel just starts the war US has to finish
US starts building first versions of stuxnet
further versions get more aggressive / noisy
2010 detected and public outlash but denial

3.7.3 stuxnet

initially detected by antivirus company in belarus
then analysed by symantec and many others
used to target nuclear facilities in iran

government backed hints
no vanity signs in the code
very well written with few bugs
20x bigger than usual, 4 0-days at the same time
cutoff date close to end of term of president

traceback
kept log of all infected pcs
hence was able to trace back to first infected pcs
were in industry companies close to nuclear facility
hence workers brought it in themselves when updating etc

target
facilities located in desert, heavily protected & airlocked
UN inspections revealed professional organisation, quality control
centrifuges spin fast to separate higher quality uran
delicate because with heat carbon shrinks but metal grows

workings
probe for siemens PLC (programmable hardware for motors) controllers
check conditions (model, arrangement known from propaganda videos)
wait for 13 days (bc timeframe to fill centrifuges)
record normal activity (to replay after getting active)
speed up by factor of 3 to make it explode
slow down to 2 herz to make it wobble and break
blocked shut down button
operators might hear difference, but could not stop it

distribution
used to be manually inserted into factory
but more and more pushed to automatic deployment
in the end, propagated self using 0-days
& stolen digital certificates from japan

builders
NSA (had the knowledge)
CIA (with the authorization via the cyber command)
8200 israel hacking group
israel pushed for more aggressive updates, distribution

updates
at first very stealthy; updating manual
got more and more aggressive with distribution
or started to shut down computers
spread to many pcs in the US too

3.7.4 USA cyber war vs iran

cyber capabilities
intransparent, but very high budget (including for offence)
only ever talked about defence
but defence knowledge can be used for offence too

stuxnet
developed under name "olympic games"
authorized by bush after PoC on real devices
then reauthroized by obama
some concerns other countries might use similar weapons
gone "rogue", spread to many pcs on the world
2012 leak said it was the US

long-term impact
nuclear reports show first fewer centrifuges
but only year after discovery recovered
now again much more centrifuges
and iran developed own cyber army

nature zeus (NZ)
much bigger program than stuxnet
designed to help against iran in case of war
like military systems, power grids, ...
possible to shut down / control without attribution

stuxnet in the US
found by homeland security
recognised risk because targeted industrial complex
but did not know it was a US weapon
never received stay down order but not informed either

iran response
biggest oil company & american banks attacked
attribution was unclear, but message of iran clear

4 einführung cyberraum

4.1 geschichte

1969 ARPANET; zivile nutzung durch forscher
1990 wird netwerk für kommerzielle zwecke nutzbar
weltweit, offen, frei als ideologie
dezentrale grundarchitektur, ausfallsicherheit
sicherheit war kein thema

4.2 architektur

server (dienstleister) - client (kunde) architektur
protokolle wie TCP, IP, HTTP, SMTP, POP, LDAP, FTP

OSI model
physical (media signal, binary transmission)
data link (physical adressing)
network (path determination to next knot)
transport (end-to-end connectivity, reliability)
session (interhost communication)
presentation (data representation / encryption)
application (network process)

4.3 informationssicherheit

schützt daten & informationen
identifiziert bedrohungen/schwachstellen
minimiert auswirkungen / eintrittswahrscheinlichkeiten
⇒ risikomanagement

CIA
confidentiality (prevent unauthorized access)
use encryption & multi-layer security
integrity (prevent unauthorized modifications)
use access control, signatures, checksums
availability (guarantee access)
use monitoring, DDoS defense, ...

risk
risko = verwundbarkeit ∗ bedrohung ∗ exposure factors
reduktion auf akzeptables level
verbleibendes risiko = risiko / kontrollen

terminologie
bedrohung als subjekt das verwundbarkeit ausnutzt
exposure factor als w'keit dass gefahr verwundbarkeit ausnützt
exploit nutzt vulnerability aus
incident wenn die bedrohung realisiert wird

threat lifecycle
threat agents gives rise to threat
threat exploits vulnerability
vulnerability leads to risk
risk can damage asset
asset causes an exposure
exposures can be countermeasured by safeguards

sicherheitslücken
häufigster fehler sind programmierfehler
programme sind umfangreich & komplex
jährliches wachstum ca 7%, viele fehler
ökonomische gründe (zeitdruck, kostendruck, fehlende incentives)

teilbereich IT-sicherheit
fokus auf IT systeme, schutz von ICT (IT assets)
braucht technische & organisatorische massnahmen

generalisierung cybersicherheit
schützt zusätzlich menschen und ihre interessen als gesellschaft
gegen angriffe auf physische gegenstände & wertesysteme schützen
inkludiert zusätzlich cyber bullying, kritische infrastrukturen
piracy als attacke auf eigentum & wertesystem "intellectual property"

4.4 hacking

inital jemand mit freude an veränderung software/hardware hat
80er jahre zunehmend negative konnotation
hacken als unbefugtes eindringen in datenverarbeitungssysteme
im strafgesetzbuch dem hausfriedensbuch nachgebildet

kategorien
script kiddies
blackhats/greyhats
kriminelle organisationen
staatliche akteure

cyber kill chain
reconnaissance (harvesting emails, personal information)
weaponization (coupling exploit with backdoor)
delivery (sending payload to victim)
exploitation (execute code on victims system)
installation (install malware on asset)
command & control (command channel for remote manipulation)
actions on objectives (hands on keyboard access)

lebenszyklus schwachstellen
3 monate suche, 1 monate entwicklung exploit
6-12 monate nutzung bis meldung hersteller
2 monate bis patch verfügbarkeit (closed source, ...)
3 monate bis patch weitverbreitet
viele vorfälle in den letzten paar monaten

schwachstellenmarkt
hacker findet 0-day + event. wirksamkeitsnachweis
whitehat nutzt bug bounty oder veröffentlichung paper
IT sicherheitsfirma informiert kunden, softwarehersteller macht patch
blackhat verkauft an 0-day broker / schadsoftware dienstleister
abnehmer sind kriminelle, militärs, nachrichtendienste, polizei

social engineering
psychologische manipulation / täuschung
zur wissentlichen / unwissentlichen preisgabe von informationen
wie phishing, help desk anrufe, physischer zugang, dumpster diving, shoulder surfing

erfolgswahrscheinlichkeit
3% basiert auch technischer sicherheitslücke
97% social engineering mit 70% erfolgsquote

häufigkeit
0-day < phishing < n-day < passwordkompromittierung
komplexität nimmt ab, mehr automatisierung

bespiele
seach engines like shodan for IoT
vulnerability scanner like Nessus
specialized OS like kali linux
social engineering toolkits like SET

5 formen von cybergewalt

5.1 verteilung von angriffen

ca 3% advanced persistent threats
etwas mehr geziele angriffe (kriminalität, aktivisten)
viele massenattacken

vergleich
schadenspotential, eingesetzte ressourcen nehmen ab
threat actors & sichbare attacken nehmen zu

5.2 konfliktformen

cybervandalismus
hacktivismus
cyberkriminalität
cyberspionage
cybersabotage
cyberterror
cyberkrieg

vergleich
häufigkeit nimmt ab
schaden, skill, benötigte organisation nimmt zu
aus incident wird campain/operation
tools sind jedoch überall etwa die gleichen

5.3 typologie angreifer

script-kiddie
(jugendliche) nutzer mit grundkenntnissen
ethik egal, gesetze unbekannt
cybervandalismus als motiv, sichtbarkeit
einzeltäter, motiviert über soziale gruppen
nutzen bestehende gebrauchsfertige tools (DoS, defacement)

hacktivist
protest / meinungsverbreitung im netz (misstände, ...)
hacker ethik, davon motiviert
nicht viele kenntnisse benötigt (aber mögl. vorhanden)
gerechtigkeit als motiv, sichtbarkeit
oft in losen gruppen organisiert
nutzen bestehende gebrauchsfertige tools (DoS, defacement)

cyberkriminelle
nutzung computer zur illegalen bereicherung
ethik/gesetze egal, kosten/nutzen logic
fähigkeiten sehr divers
finanzielle bereicherung als motiv
einzeltäter, heute often organisiert
nutzen social engineering, botnets, APT
inkl. wirtschaftsspionage

cyberspion
nutzung computer zum stehlen wertvoller daten
ethik egal, gesetze teilweise
fähigkeiten relativ hoch
finanzielle / strategische bereicherung
teil organisierter kriminalität, nachrichtendienst
nutzen social engineering, exploits, APT

cyberterrorist
effekte des hacks entsprechend terroranschlag normaler raum
ethik/gesetze egal, kosten/nutzen logic zur kommunikation
relativ hohes technikwissen
politische motivation / kommunikation als motivation
teil terroristischer gruppierung
nutzt defacement, DDoS attacken, exploits, APT

cyberkrieger
nutzt computer zur erreichung operativer/strategischer ziele
kriegsvölkerrecht teilweise relevant, kosten/nutzen zur strategie
hohes technisches wissen, kombiniert mit geheimdienstlichen infos
politisch-strategische motive
im staatlichen dienst (armee, geheimdienst)
nutzt defacement, DDoS attacken, exploits, APT
vs cyberterrorist der teil einer terroristischen vereinigung ist

5.4 schäden

subjekte
nationen (economy, security, society, international relations, ...)
infrastructure (transportation, power, communicaton)
organisations (comapny, schools, NGO, hospitals, ...)
individuals (CEO, doctors, children, pensioner)

arten
physical (bodily injury, property damage)
political (electoral system, loss of trust)
psychological (depression, panic, stress)
reputational (consumers go, relations suffer)
economic (financial / job loss)
cultural (loss of communication means, societal values)

direkt vs indirekt
ICT kann direkt schäden anrichten (ursprung, unterstützung)
ICT möglicherweise auch das ziel des schadens
indirekt schäden hervorrufen (dominoeffekte)

5.5 cyberkrieg

strategischer cyberkrieg
attacker gegen staat/gesellschaft um verhalten zu ändern
ziel sind kritische infrastrukturen
hat so noch nie stattgefunden

operationeller cyberkrieg
zur unterstützung physischer militärischer operationen
ziel sind militärische datenströme, einrichtungen
findet sehr oft statt

cyberwaffen
analogie zu realer waffe nicht so zutreffend
da kein richtiger "trigger"
besser "software" zu verwenden

krieg vs kriminalität
cybercrime vs cyberwar unterscheidung wichtig
da verfolgung unterschiedlich ist

talinn manual
definiert anwendung völkerrecht im cyberspace
analogie zu kinetischen mitteln
"... result in death, injury, significant destruction"
anforderungen sehr hoch gehalten
zB russische einflussnahme in US wahlen 2016 weit unter definition

5.6 schwierigkeiten

attribution
eindeutige quelle / motivation oft unklar
massgebliche voraussetzung für selbstverteidigung
forensik braucht zeit, nicht immer erfolgreich
ergibt politischer spielraum zur attribution (oder eben nicht)

payload-problem
unterschiedliche versionen von malware
schwierig zerstörungspotential einzuschätzen
spionage/sabotage gleiche tools, nur unterschiedliche motivation

5.7 aufwand

voraussetzungen
aufklärung/spionage im vorfeld nötig
unbekannte sicherheitslücken (zero-days)
programmierung von prof. expliots
angriff beständig halten

zusätzliche schwierigkeiten
ab 1stem angriff vorteil beim verteidiger
lebensspanne zero-days kurz (500 stunden)
entwicklung sehr langwierig (2-5 jahre)

6 strategische kommunikation & manipulation

6.1 geschichte

kalter krieg mit antagonisten (bipolar)
post-kalter krieg; unklar was kommt (unipolar)
war on terror; westen vs islamismus (multipolar)
heute westen vs RU/CN (multipolar)

6.2 strategische kommunikation

strategische narrative
selbstdefinition als was man empfunden werden möchte
abgrenzung zu anderen
über medien, politiker, informationskontrolle, ...

strategische kommunikation
verbreitung strategischer narrativer (über statements, ...)
kontrolle anderer infos

6.3 diffusion von CN/RU technologien

chinesische technologien in china
russische technologien in russland
auf der ganzen welt verbreitet
USA beides, EU vor allem china

6.4 idealtypisches modell zur meinungsbildung

evidence entsteht
experten beurteilen diese beweise
eliten / offizielle bewerten wiederum experten
medien / kulturen greifen es auf
individum beeinflusst von spheres
public sphere (medien / kultur)
social sphere (private kontakte)
para-social sphere (einseitige beziehung zB promis)

einwirkung
forging / leaking fakten
experten credibility verstärken / vermindern (trolling, flaming)
deceptive identities (sich als fake offizielle ausgeben)
fake news / fake media
public sphere wird mit botnets / malign rhetorics / memes beeinflusst
social phere mit cognitive hacking
para-social hacking (person existiert gar nicht)

6.5 einflussoperationsstrategien

astroturfing (fake "community" erstellen; mögl. bezahlen)
point & shriek / black propaganda (fakten erstellen & skandal erzeugen)
laundering (legitimize dark evidence)
flooding (zu viel informationen macht eine einordnung unmöglich)
cheerleading (overflowing information space to hide relevant info)
raiding (information surge for short time)
polarization (sides radikalisieren)
hack, mix, release (hacken, anreichern, in die öffentlichkeit bringen)

6.6 kontrollierbarkeit & effektivität

wie kann operateur die strategischen effekte kontrollieren
gegenreaktion/vergeltung könnte zu gross ausfallen

beispiele
russland motiviert protesters in der USA

6.7 strategie der schweiz

naturalisierung vs konfrontation
ignorieren vs blockieren
schweiz eher naturalisierend, ignorierend

andere mögliche vorgehensweisen
zivilgesellschaft
fakten
kollaboratives vorgehen
gegennarrative
gegenpropaganda
schwellenwert erhöhen
ignorieren
regulierung einsetzen
proaktiver staat führt information operations durch

6.8 einschätzungen

wer legt normen fest / verhindert manupulation
⇒ zivilgesellschaft (wie DE) vs staat (wie FR)

zentrale unterschiede
was geschützt werden soll (industrie, meinung, stabilität, rechte)
welche mittel verwendet werden dürfen (überwachung, zensur, vergeltung)

liberale demokratien
erlauben diskursiver wahrheit

jedoch soll trotzdem vor angriffen geschützt werden

6.9 eurpoäische strategien entgegen russischer einflussnahmen

russland verbreitet eigenen standpunkt inkl. desinformation
mit eigenen medien, trollfabriken, youtube channels, parteispenden

confronting
nach aussen gerichtet, inkl im land des gegners
gegen-positionen verbreiten anhand des ursprünglichen narrativ
wie estonian russian TV für eigene russische minderheit
aber entspricht den gleichen taktiken die verurteilt werden

blocking
nach innen gerichtet
positionen des gegners blockieren, zB durch zensur
wie latvia russia today blockiert hat
aber undemokratisch (zensur), einfach umgänglich

naturalising
nach aussen gerichtet
eigene positionen verbreiten (ohne andere explizit anzugreifen)
wie deutschland transparente information "vorsprung durch vertrauen"
aber könnte dennoch als agressiv aufgefasst werden

ignoring
nach innen gerichtet
position des gegeners ignorieren; vertrauen in institutionen hoch
wie schweden
aber möglicherweise unrealistisch

optimale strategie
"othering" sollte vermieden werden
demokratische werte sollten bewahrt werden
dementsprechend naturalising & ignoring die vielversprechendsten

7 subversion & machtpolitik

7.1 politische macht

jemand zu etwas bringen was dass er sonst nicht tun würde

gewalt
materielle kapazitäten den gegner zu etwas zu bringen
oder materielle kapazitäten des gegners kaputt zu machen

demokratie
durch verhandlungsgeschick und überzeugungskraft
gewinn des besseren arguments vs drohungen / abschreckung

7.2 theorien der cyberpower

kuehl
ausnutzung umgebung wie bei anderen dimensionen
als designed environment
als neue form der gewalt

nye
ability to obtain preferred outcomes
through electronically connected resources
wie kuehl, aber included auch soft power

betz & stevens
neues operatives (aber nicht strategisches) umfeld
akteure bewegen sich in vorgegebenen umfeld
können es aber auch selber ändern (wiederspruch)

zusammenfassung
produzierung physischer effekte schwierig (krieg)
verdeckte interaktion verhindert signale (diplomatie)
stattdessen klare parallelen zu geheimdienstoperationen
jedoch müssen diese wiederum ohne macht auskommen

7.3 subversion als machtform

unterwanderung systeme & übertragung macht auf sponsor
stille alternative zur gewalt mit strategischem potential
aber begrenzt durch operative nachteile

olsson
secret political actions against rules/norms
by ignoring/violating then
to harming institutions

definition
strategisch (kapazitäten unterwandern)
operativ (schwachstellen verwenden)
wie infiltration politische berater, kritischer infrastrukturen

characteristika
vesteckt (sowohl ziel als auch urheber)
indirekt (nutzt system des gegeners)
ausnutzung von schwachstellen
nicht gewalttätig

strategische vorteile
wenig risiko (versteckt, plausible deniability)
geringe kosten (da material gegners genutzt wird)
sieg ohne krieg (militär muss nicht eingesetzt wird)

operative nachteile
langsam (identifikation & nutzung vulnerabilities schwierig)
geringe intensität (je stärker effekt, desto höher hürden)
unzuverlässigkeit (abhängig von system des gegners, testen schwierig)

7.4 cyber power als subversion

unterwanderung computer system (statt sozialer)
strategisches versprechen (sieg ohne krieg)
jedoch operative einschränkungen

soziotechnische systeme
zusammenspiel hardware, software, benutzer
soziale prozesse (austausch, dating, networking, ...)
physisch (internet of things)
wirtschaft (aktienhandel, ebanking)
mehr convenience, aber grössere verwundbarkeit

verwundbarkeiten
soziale verwundbarkeiten um zugriff zu erhalten
wie menschliches verhalten, sicherheitpraktiken
technische verwundbarkeiten um unerwartete effekte zu produzieren
wie schwachstellen in hardware / software

subversionsprozess
zugriff und kontrolle über system als ziel
zu beginn oft nur einziges gerät infiziert
danach ausweitung, vertiefung kontrolle ("lateral movement")

verdeckte vorgehensweise
erst nach aktivem effekt bemerkt opfer infiltration
urheber kann sich danach bekennen

indirekte effekte
zugang braucht eine existierende schwachstelle
effekte werden durch kompromittierte system prodziert
systeme müssen daher verfügbar & tief eingebettet sein

ressourcen
zeit (aufklärung, entwicklung)
fachwissen (entwicklung exploits, vermeidung entdeckung)
kreativität (zielfindung, vorgehensweise)

strategisches potential
geringes risiko (covert)
geringe kosten (minimaler materialeinsatz)
sieg ohne krieg (strategischer vorteil ohne krieg)

operative einschränkungen
langsam (vulnerability, exploits, ausbreitung)
geringe intensität (abhängigkeit zielsystem)
unzuverlässig (zielsystem unbekannt / testen nicht möglich)

operative vorteile
grosse skalierbarkeit (wie selbstreproduzierbarkeit)
skaleneffekte (gerine zusätzliche kosten pro zusätzlichem system)

7.5 offense, defense & deception in cyber space

not much empirical activity in cyber offense
but deception has become easier with cyber space
limits at the same time attacker capabilities (to avoid detection)

deterrence
does not work same as with conventional weapons
rationality (as might be script kiddy attacking)
attribution (as unclear who exactly attacked)
secrecy (tools can only be used onced, then 0-day fixed)

defense
weakest link problem
defense cost rises much faster than attacker cost

past offense actions

most "attacks" simple probing of networks
espionage & real attacks small & regionally constrained

deception
hiding is easy
combine vulnerable machines & gullible users
protection of both negates usefulness of computers
use dissimulation (hide truths) and simulation (show myths)

8 fallstudie ukraine

8.1 konflikt

seit 2013
hybride kriegsführung / asymmetrischer konflikt
über 8 jahre fanden 5 grosse cyber aktionen statt

beginn
ukrainisches parlament beschliesst eu beitrittshandlungen
russland fürchtet verlust aus einflussbereich
2013 nach putin/ukraine werden verhandlungen eingestellt
stattdessen einbettung in eurasian customs union

euromaidan proteste
nov 2013 - feb 2014 dauern über monate an
mit zunehmender gewaltanwendung
22. feb tritt yanukovych zurück & flieht nach russland

übernahme krim
pro-russische proteste ab 23. februar
koordinierte übernahme krim militärbasen und regierungsgebäuden
referendum im 16. märz für russische übernahme
"offizielle" annektion ein bisschen später

übernahme donbass
gleiches schema wie krim
jedoch unvollständige kontrolle, widerstand in bevölkerung
ukraine startet militärische gegenoffensive
offener krieg ohne klare gewinner bis heute (2020)

fazit
ukraine verfolgt weiterhin pro EU kurs
aber signifikante strategische gewinne (krim)
keine cyber-operationen vor ausbruch militärkonflikt

8.2 cyberoperationen.

8.2.1 wahleinmischung mai 2014

wahlen nach der übergangsregierung der protestbewegung
computersystem zentraler wahlkommunikation bricht zusammen
CyberBerkut bekennt sich; APT 28 wahrer verursacher
koordination mit staatsmedien & propagandawahlen
im sinne von "elections are rigged" von der USA
backups bringen system nach 20h wieder online

fazit
relativ kurze entwicklungszeit
geringe intensität (backups vergessen)
strategisch irrelevant; es wird pro-EU gewählt

8.2.2 stromunterbruch dez 2015

pattsituation an der front
strom wird unterbrochen für 250k personen in ruraler region

vorgehen
erste infiltration 12. mai 2014 (19 monate entwicklungsdauer)
phishing email mit anhang
stromanbieter entdecken präsenz unternehmen jedoch nichts
windows & industrial control system 0-day
infiltration aus firmennetz zu industry system

mechanismus
manuelle eingabe von störbefehlen über herkömmliche UI
unterbruch des physikalischen prozesses

abwehr
opfer können auf manuelle kontrolle umstellen
nach 6h attacke bereits nutzlos

fazit
keinen einfluss auf front / demokratie
wirtschaftlicher schaden sehr gering
psychologisch auch (da stromausfälle häufig sind)
kein messbarer einfluss auf konflikt

8.2.3 stromunterbrucht dez 2016

strom wird unterbrochen für einige mio personen in hauptstadt
nach 75 minuten bereits behoben (umstellung manuelle kontrolle)
keine erkennbare koordination zu konflikt

fazit
lernprozess aus vorheriger attacke
hätte kraftwerk beschädigen können
jedoch IP adresse falsch eingegeben
daher keine weiteren effekte

8.2.4 NotPetya juni 2017

randsomware im ukrainischen privatsektor
geschäftsleben wird lahmgelegt (inkl. ubahn, flughafen)
danach ausbreitung weltweit (inkl. russland)
keine erkennbare koordination zu konflikt

entwicklung
dez 2016 moonraker worm zur reproduzierung
märz 2017 ausbreitung durch softwareupdates
mai 2017 buchhaltungssoftware medoc ukraine kompromittiert
juni 2017 netpetya malware in update medoc
fünf tage später aktivierung des verschlüssungsmodul

verwundbarkeiten
alter, ungepatcher server
kunden vertrauten softwareanbieter
automatische updates praktisch

fazit
wirtschaftliche konsequenzen für firmen
schaden für ukraine (0.5% BIP), 10 mia weltweit
starker psychologischer effekt, medienaufmerksamkeit
grosser kollateralschäden (mehrere millionen systeme)
aber kein klarer einfluss auf konflikt, sanktionenpacket motiviert

8.2.5 BadRabbit oktober 2017

randsomware, jedoch lassen sich daten wiederherstellen
virus in flash-player update
viel weniger systeme wie NotPetya (mehrere hundert)
zuverlässiger (kein kontrollverlust, vorzeitige entwicklung)

fazit
unklarer militärischer fortschritt / schädigung demokratie

8.3 fazit

irrelevant in militiärischer / demokratischer dimension
trotz vieler jahre entwicklungszeit sehr wenig einfluss
bei grossem effekt kontrollverlust (NotPetya)
keinen beitrag zu russischen strategischen zielen

9 attribution

9.1 MH17 (flugzeug ukraine)

wo (klar sichtbar)
wann (absturzzeit)
wie (burk-rakete)
wer (herausgefunden mit telefonaufzeichnungen)
warum (absicht, autorität)
mehrere quellen für alles

9.2 formen von attribution

maschine, mensch der diese bedient, verantwortliche partei
geographischer ort, täter, verantwortliche partei
taktisch (was & wie), operativ (wer), strategisch (warum)

9.3 möglichkeit der attribution

täuschung skaliert nicht
soziale verhaltensmuster durch gewohnheit
effizienz (rückverfolgung als resultat tradeoff)
besonders schwierig bei einfachen/einmaligen & sehr professionell
manchmal nicht möglich

9.4 aspekte aus angreifersicht

gewollte attribution
wann & in welchem ausmass

grosse unsicherheit
komplexe opfer sind einfache ziele
aber schwierig sämtliche spuren zu verwischen

mögl. absichtliche beeinflussung
opferstruktur vermischen (auch non-targets, targets des gegners)
wiederverwendung code / infrastruktur anderer akteure

9.5 attribution

als prozess
kostet geld, zeit, ressourcen
genauigkeit ist eine politische / effizienz / vorbereitungsfrage

9.6 angriffsinfrastruktur

adversary space mit attacker & kontrollierender organisation
target space mit opfer & kontrollierender organisation
dazwischen neutral space mit personas, websites, relay servers
schwierigkeit neutral space zu durchqueren

9.7 taktische attribution (was & wie?)

verhalten (routine, lernmuster, fehler)
angreiferabsicht (will attribuiert werden)
effizienz/risiko tradeoff
diverse beteiligte disziplinen
je nach angriffsart attribution grundsätzlich einfacher

details
indicators of compromise (IOC) springen an
angriffsvektor feststellen (wie eingedrungen)
targetinganalyse (was ist das ziel)
laterale bewegungen (was noch alles betroffen)
exfiltration (wenn attacker daten extrahiert zu sich)
infrastrukturanalyse (was hat angreifer für infrastruktur)
modularität/code (wird ähnlicher code woanders verwendet)
funktionalität (was kann der code? zero-days?)
cluster (ähnliche tools zusammennehmen)
sprache (was ist die muttersprache)
personas (wurden handles bereits einmal verwendet)
lebensmuster (korrelationen mit arbeitszeiten & feiertage)
kompromisse stealth/speed
genehmigung (feature flags zeigen rechtliche/bürokratische struktur)
fehler (durch komplexität, vanity, gewohnheiten)
tools (telemetrie, weitere daten aus anderen bereichen)

9.8 operative attribution (wer)

diverse beteiligte diszipinen & quellen
hypothesen (aus technischer analyse & weiteren quellen)
umfang (opfercharacterisierung & deren zeitliche veränderungen)
stufen (ob selber ziel oder um kunde anzugreiffen)
evolution (korrelation zeitlicher änderungen mit geopolitik)
angreiferkommunikation (direkt / indirekte kommunikation)
insider-unterstützung (wissentlich / unwissendlich)
intel (inwiefern angreifer insiderwissen genutzt hat)
kosten (welche resourcen wurden eingesetzt)
bedeutung (welches arsenal wurde verwendet)
geopolitischer kontext (regionales/historisches verständnis)
kompetenzen (verwendete resourcen)
doxing (verknüpfung erkannte personas mit organisationen)
organisationen/tasking (timings von aktionen)
konkurrierende hypothesen abwägen

9.9 strategische attribution

frage nach ziel, erfolg, schaden, konsequenzen
durchgeführt von führungskräften, entscheidungsträger, analysten
katz und mausspiel mit verwendeten werkzeugen, aufgedeckten fehlern
private erstellen clusters, staaten ordnen cluster zu

9.10 attribution kommunizieren

veröffentlichung ist kostspielig
als teil der antwort auf einen vorfall
mit community, gegner, öffentlichkeit teilen

evidenzstandards
für innerstaatlich reicht überzeugender verdacht
keine internationalen standards zur beweisführung
geheimdienst urteilt anhand w'keiten & vertrauenswürdigkeit quelle

zielgruppenspezifisch
sense-making legt fest was passiert ist (technisch)
durch staat, private, geheimdienste
meaning-making kommuniziert befunde & deren interpretation (politisch)
an öffentlichkeit inkl. verbündete/inland/drittparteien/gegner
folgt oft bereits etablierten geheimdienstprozessen analog anderer quellen

arten der attribution
diplomatische erklärungen / erklärungen des präsidenten
autorisierte leaks / einsendungen an virustotal / ...
gerichtsfälle / staatliche erklärungen

verwendung öffentlicher attribution
gestaltung betriebsraum (gewohnheitsrecht für gegner/drittstaaten)
"erlaubtes" wird nicht attribuiert (tacit collusion)
bekämpfung von bedrohungen (tools unbrauchbar machen)
innenpolitik (bildung, krisenmanagement, ...)

attribution durch industrie
für marketing / reputationsgewinn
methodiken zum teil schwach / ohne ethische richtlinien

qualitativ hochwertiger report
klares attributionsobjekt (tools, entwicker, betreiber, kampagne, gegner)
reproduzierbare beweise & quellenvielfalt
annahmen explizit/implizit geklärt
klärung schwachstellen in beweisführung & alternative hypothesen
berichte je nach zielpublikum mit konfidenzniveaus

10 was ist der staat

10.1 elemente des staat

staatsgewalt
polizei (innen)
militär (aussen)

gewaltentrennung
gericht (judikative, gesetztgebend)
regierung (exekutive, ausführend)
parlament (legislative, rechtssprechend)

staatsgebiet
grenzen

staatsvolk
in sektoren (staat, wirtschaft, gesellschaft)
rechte & pflichtenteilung
"gesellschaftsvertrag" nach rousseau
begründet durch gemeinwillen des volkssouveräns

10.2 sozialer wandel

ausdifferenzierung gesellschaftsformation
zu wechselseitiger abgrenzung
⇒ militärstaat (behauptet staatsgebiet / reichtum)

ablösung feudalsystem
zu kapitalistisch-marktwirtschaftlicher herrschaft
⇒ polizeistaat (schutz mächtiger/reicher vor untertanen/armen)

ausbau demokratischer strukturen
zu gewahltentrennung, transparenz
⇒ rechtsstaat (garantiert anspruchtsrechte untereinander / zu staat)

hochzeit industriegesellschaft
zu wohlstandsinseln
⇒ sozialstaat (sicherung / verbesserung lebensgrundlagen)

übergang informationsgesellschaft
zu globalisierung
⇒ deregulierter staat (governance statt government)

11 rollen des staates in der cybersicherheit

aushandlung unter staaten (internationale normen)
aushandlung innerhalb unterschiedlichen bürokratischen einheiten
legt rollen, verantwortlichkeiten, verhaltenregeln, gesetze fest

11.1 evolution

1980er
limitiertes problem
klassifizierte daten sollen geschützt werden
staat als eigentümer

1990
zunehmend vernetzte systeme
kritische infrastrukturen sollen besser geschützt werden
staat als eigentümer & problemverantwortlicher

2000
zunehmend bekanntes problem
cyber-wettrüsten & gezielte angriffe der nachrichtendienste
staat als eigentümer, verantwortlicher und urheber des problems

11.2 sicherheitslogiken

nach aussen
suche nach kooperation, jedoch nicht bei nationaler sicherheit
machtausbau mit cybermacht (regulationen unerwünscht)
sicherheitsdilemma, wettrüsten (regulationen erwünscht)

nach innen
ökonomische dimensionen im vordergrund
schutz kritischer infrastrukturen
aber liberale marktordnung

11.3 rollen des staates

garant / beschützer (sichern eigener ziviler/militärischer netze)
gesetzgeber / regulierer (schaffung rechtlicher grundlagen)
unterstützer/vertreter gesamtgesellschaft (rahmenbedingungen wirtschaft/gesellschaft)
partner (public private partnerships)
wissensschaftler und -verbreiter (awareness, sensibilisierung, ausbildung)
unsicherheitsproduzent (national vs information security / privacy)

11.4 interessenskonflikte

gruppen innerhalb staat/gesellschaft/wirtschaft bilden interessensgruppen
zielkonflikte (schwachstellenproblematik für strafverfolgung vs sicherheit)
macht abhängig von stärke interessensgruppe und historischen rollen/vertrauen

fragen
grenze der verantwortung (staat vs gesellschaft vs gsellschaft)
kompetenzen zur wahrnehmung verantwortung (welche mittel einsetzbar)

spannungsfeld staat-wirtschaft
sicherung kritischer infrastrukturen
negatives entschärfen aus globalisierung, privatisierung, liberalisierung ohne vorteile daraus zunichte zu machen
vertrauen in wirtschaft/staat vs regulierung
wirtschaftliches handeln vs resilienz / widerstandsfähigkeit

spannungsfeld staat-gellschaft
sicherheit & freiheit im digitalen raum
"leidensdruck" tief; sicherheitsempfinden bereits relativ hoch
fraglich inwiefern höhere kosten / regulierung akzeptiert wird
polizeiliche/geheimdienstliche befugnisse vs privacy/anonymity

spannungsfeld gesellschaft-wirtschaft
rahmenbedingungen schaffen für sicherheitsökosystem
balance / sensibilisierung von funktionalität vs sicherheit
verpflichtungen der dienstleistungsanbieter
rechtliche rahmenbedingungen (inkl. global)
konsumentenschutz bezüglich daten und monopole

11.5 paper

theoretisch (wie staat in literatur)
portraitierung als sicherheitsakteur zu eingeschränkt

empirisch (wie staat policies entwickelt)
entspricht wie er von aussen wahrgenommen wird / sich selbst sieht
security guarantor (secure own systems)
legislator / regulator (clarify hierarchy)
supporter/representative of society (advance international law)
security partner (PPP provide protection)
knowledge generator/distributor (trustworthy source of information)
threat actor (misuser of knowledge)

normativ (wie sich staat verhalten sollte)
sicherung der kritischen infrastrukturen mit wirtschaft
sicherheit/freiheitsabwägung gesellschaft
sicherheitsecosystem sollte kuriert werden

wesentliche fragen
verantwortlichkeit statt/wirtschaft/zivilesellschaft
kompetenzen um diese verantwortung wahrzunehmen

12 voraussetzungen staatlicher cyberfähigkeiten

12.1 cybersecurity capacity maturity model (CMM)

zur beurteilung von staaten
unterteilt in faktoren, die aus aspekten bestehen
aspekte bestehen aus indikatoren, die bewertet werden
bewertung in start-up, formative, established, strategic, dynamic

beispiel
legal frameworks als faktor
legislative framework for ICT security als askpekt
"efforts to draw attention" → startup
"experienced stakeholders consulted" → formative
"frameworks adopted" → established
"review of existing legislation" → strategic
"mechanism to harmonize" → dynamic

stakeholders
cyber task force
private sector & business
critical national infrastructure
legislators / policy owners
government ministries
defence / intelligence community
criminal justice / law enforcement
academia, civil, society groups & internet governance
international partners

12.2 CMM faktoren

cybersecurity policy & strategy
nationaly cybersecurity strategy
incidence response (identifizierung, meldestellen, ...)
critical infrastructure protection
crisis management (etablierte prozesse)
cyber defence
communication redundancy

cyber culture & society
cybersecurity mind-set
trust & confidence on the internet
user understanding of personal information protection online
reporting mechanisms
media and social media (aufarbeitung wissen)

cybersecurity education, training and skills
awareness raising (insb. besonders exponierte)
framework for education (lehrpläne)
framework for professional training

legal and regulatory frameworks
legal frameworks
criminal justice system
formal & informal cooperation frameworks to combat cyber crime

standards, organisations, and technologies
adherence to standards
internet infrastructure resilience
software quality
technical security controls
cryptographic controls
cybersecurity marketplace
responsible disclosure

12.3 anwendung CMM

im zeitlichen verlauf
daten aus 2015 und 2018 mit CMM
meiste askpekte im startup - formative bereich
fortschritte sichtbar, jedoch durchschnittlich nur 0.2 (aus 5)

ziel
zu einschätzung wie effizient gewirtschaftet wurde
und in welche bereiche investiert werden sollte

resultate
mindset in staaten weniger verbreitet wie bei privaten
weil diese mehr existentielle gefahren haben

datenerfassung
möglicherweise nicht alle daten geteilt

auswertungen
aspekte miteinander vernetzt; verstärken sich mögl. gegenseitig
zur evaluation nationaler stärken & schwächen

zur identifizierung regionaler champions & best practices

12.4 voraussetzungen zum ausbau

verbesserung im cybersecurity-mindset der regierung
institutionalisierte koordination (inkl. regelung nachfolge)
EU NIS-richtlinien, DSGVO als best practices
standards & zertifikate in ermangelung von lernplänen
informelle zusammenarbeit zum schnellen/flexiblen informationsaustausch

12.5 grossbrittanien

nationales cybersicherheitscenter
um ressourcen zu poolen, skaleneffekte
um flexibler für grössere zielgruppe verfügbar zu machen

12.6 paper

many entites involved in defense of cyber acitivies
like state / private, civil / military
major and minor seams between entities
the bigger the seam the more ineffective the response
with improper response, escalation potential exists

examples
mariposa botnet (state intransparency motivated privates to take action)
BGP routing errors resolved using professional network
russian election hacks could not properly defended against
SPE hack worked on some levels, on some not

13 cybersicherheit und kritische infrastrukturen

schutz kritischer infraskturen (SKI)
in der schweiz durch bundesamt für bevölkerungsschutz (BAPS)

13.1 definition

prozesse, systeme, einrichtungen
essentiell für funktionieren wirtschaft / wohlergehen bevölkerung

interpretation
wirtschaft als primär schützenswertes objekt
"wohlergehen" inkludiert nationale sicherheit

umsetzung
massnahmen zur reduktion eintrittswahrscheinlichkeit
und verminderung schadensausmass
von störungen, ausfällen oder zerstörungen

sektoren
unterteilt in 9 sektoren, 27 (wirtschafts-) branchen
behörden (forschung/lehre, kulturgüter,
parlament/regierung/justiz/verwaltung)
energie (erdgas, erdöl, fern & prozesswärme)
entsorgung (abfall, abwasser)
finanzen (dienstleistungen, versicherungen)
gesundheit (chemie/heilmittel, labor, medizinische versorgung)
information (IT-dienstleistungen, medien, post, telekommunikation)
nahrung (lebensmittel-/wasserversorgung)
öffentliche sicherheit (armee, polizeit/sanität/feuerwehr, zivilschutz)
verkehr (luft, schiene, schiff, strasse)

methode
erstellung geheimer inventarliste durch bund und kantone
einbezug spezialisten aus firmen um prozesse zu verstehen
bezeichnung der relevanten objekte
festlegung von kriterien nach objekten
beurteilung kritikalität der objekte

beurteilung kritikalität
BAPS risikoanalyse kriterien / internationale angewendet
auch politischer einfluss bei anwendung definitionen
> 10% versorgung bürger mit wichtigen gütern
> 5% anteil an funktion kritischer infrastruktur
> 10 todesopfer bei freisetzung substanzen
wenn strategisch wichtige funktion

vision resilienz
ausfälle möglichst verhindern (widerstand)
bei ausfällen schadenausmass gering halten (anpassung / adaptation)
und wieder erholen (regeneration / bounce back)

bounce-back vs adaptation
bounce-back eher technisch (stromnetz zurück online)
adaptation eher systemisch (gesellschaft passt sich an)

13.2 historischer kontext

schutz kritischer infrastrukturen aktueller schwerpunkt debatte
ausnutzung verwundbarkeitein durch böswillige akteure

SKI als sicherheitsansatz
beschäftigung mit kritischen systemen
identifikation verwundbarkeiten und resultierende bedrohungen
techniken zur reduktion der verwundbarkeiten

strategic bombing (nach 2WK)
gezieltes ausschalten von wichtigen industrieknoten
double-edged sword durch zunehmende industrialisierung
strategic bombing survey erfasste KI

standartisierung techniken (60-70er)
total preparedness (gesamt-gefahrenplanung)
non-deterrable threats (auch nicht-staatliche akteure)
virtal system security (etablierung als eigenständiges problem)

informationssicherheit (80er jahre)
neues technisches vokabular und analytische tools
weg vom militärischen fokus / physischen objekten
zu wirtschaft / gesellschaft & informationsobjekten

13.3 sicherheitsdefizit

wirtschaftliche überlegungen vs nationale sicherheit
führt zu sicherheitsdefizit bei privatisierten sektoren

staatliche eingriffe
staat greift in markt ein zur behebung marktversagen
erlass von geboten & verboten
steuerung durch staatliche einnahmen / ausgaben & totaler geldmenge
einfluss durch aussenwirtschaftliche beziehungen (zollabkommen, ...)
verstaatlichung / privatisierung / public private partnerships
zur stabilisierung, steuerung, umverteilung

problem regulierung
"compliance behavoir" (exakte befolgung ohne common sense)
hohe diversität, komplexe standards, unklar wann "genug"
"threat of regulation" führt zu selbstregulation

versicherungen
wenig verfügbare versicherungen für cyber-risiken
weil abschätzung risiko schwierig
weil verursacher kriminell / mögl. staatlich motiviert

public private partnerships (PPP)
zusammenarbeit staat & private akteure
informationsaustausch über incidents & gegenmassnahmen
frühwarnungen (zB durch melani, "allgemeine wetterlage")
gegenseitige unterstützung bei incidents
strafverfolgung der angreifer
gemeinsame finanzierung forschung & sensibilisierung
gemeinsame policy-entwicklung und strategiebildung

limitierungen PPP
unklare rollen & verantwortungen, falsche erwartungen
mangelndes vertrauen, divergierende interessen
frustrationsgefahr (ineffizient, kooperationsmangel)

weiterentwicklung PPP zu meta-governance
PPP müdigkeit (zu langsam, ohne klares ziel)
austausch in denen staat nicht als partner sondern facilitator auftritt
wie meta-governance; staat übernimmt koordination / stimulation
homogene selbstorganisierende netwerke überwachen sich selber
genügend expertise und überlappende interessen

13.4 paper

information sharing is essential
only question is how to organize it

firms vs state
different interests
for example missing confidentiality could cause reputation issue
complex coordination with different state entities

self-organizing network
state will no longer define, but simply facilitate networks
will still observe if networks fulfil its purpose (self-regulation)
more natural common grounds between companies
better scalability
easier cooperation for international firms

but responsibilities even less clear

14 kriegsvölkerrecht und andere normen

14.1 normen und regime

struktur
prinzipien (gemeinsame grundannahmen)
normen (allgemeine verhaltensstandards)
regeln (spezifische verhaltensvorschriften)
verfahren (gemeinsam vereinbarte prozeduren)

regimetheorie
zwischen / über staaten herrscht anarchie (da keine weitere macht)
aber normen / regelgeleitete formen der kooperation

normen
verhaltensorientierte regeln (definiert durch soziale sitation)
erwartungen (hinsichtlich handeln / nichthandeln)
wertebasiert (von überwiegender mehrheit gesellschaft getragen)
formell (gesetzte, ...) / informell ("normal")
kann (soziale gewohnheiten) / soll (bräuche) / muss (rechtlich)
zur orientierung im alltag (eigener/fremder aktionen)
verinnerlicht (glaube an legitimität) oder angst vor betrafung
durch vorhersehbares verhalten orientierung im alltag möglich
gebunden an bestimmten gesellschaftlichen zusammenhang, veränderlich

lebenszyklus normen
entstehung (entrepreneurs überzeugen aus altruismus & idealismus)
kaskade (staaten/NGOs institutionalisieren durch legitimität & reputation)
internalisierung (bürokratie/anwälte institutionalisieren zur konformität)

regime
basieren auf / benötigen normen
transparenz, stabile erwartungen & geringe transaktionskosten
insitutionelle bearbeitung von problemlagen
kooperationsbereitschaft erhöht sich auch in anderen bereichen
no vs tacit regime (low formality & low vs high erwartungen)
dead letter vs classic regime (high formality & low vs high erwartungen)
regeln durch verhaltensweisen, markt, gesetze, technologien

14.2 cyberspace

generell wenig normen in sicherheitpolitik ("high-politics" → wenig grundvertrauen)

regime
komplexer als andere bereiche zB nuklearwaffen
weil nicht-staatliche akteure, dynamische entwicklung, multidimensional
dennoch bereits etablierte normen, weitere verfestigung realistisch

layers
economical / societal (education, industry, trade, media, finance, health)
norms by WEF, W3C, governments, private sector, NGO, academia
local (root services, domains, IP addresses, protocol parameters)
norms by ICANN, IETF, ISO, TLD operators, DNS, IEEE
infrastructure (internet exchange points, cables, satellites)
norms by GSMA, IEEE, national regulators

societal layer
content (content policy, public good, hate speech, social media, ...)
security and trust (crypto, cybersec, hacking, surveillance)
commerce (intellectual property, jurisdiction, consumer protection)
access (cloud computing, right to access, capacity development)

14.3 normierungsbestrebungen cyberspace

die meisten bestrebungen post-stuxnet zur deeskalation / stabilisierung
staatlich als auch nicht-staatliche

art 51. UN charta
kriegsvölkerrecht (klärt jus ad bellum, "wann erlaubt")
recht auf individuelle / kollektive selbstverteidigung
unter einhaltung prinzip proportionalität / notwenigkeit
stuxnet wurde teilweise als angriff gemäss Art. 51 angesehen
cyber-angriffe jeweils unterhalb schwelle UN charta, grauzone

UNO normierung durch UNGGE
um grauzone der cyber-angriffe auszuleuchten
vereinbarung "voluntary, non-bindung rules for responsible behaviour"
um sichere ICT umwelt zu erreichen
2015 verfassung consensus report (völkerrecht anwendbar)
2017 keine einigung
unklarheit anwendbarkeit selbstverteidigung, humanitäres völkerrecht
unterteilung in zwei working groups (mächtige, der rest)
dadurch schwächung des weiteren prozesses

talinn manual (2013)
motiviert aus 2007 angriffe estland, 2011 stuxnet
2009 verfasst zu interpretation völkerrecht im cyber-space
fokussierung auf incidents die krieg gleich kommen (cyber warfare)
2013 veröffentlicht
einfach verständliches handbuch inkl. erklärungen
jedoch aus westlichem blick (keine gemeinsam geteilte norm)
jedoch fokussierung auf cyber krieg (daher ohne beispiele)

talinn manual 2.0 (2017)
änderung auf cyber operations
jedoch unklar was für recht überhaupt zutrifft
jedoch fokus wiederum nur auf staat vs staat

initiativen von unternehmen
2017 digital geneva convention (microsoft)
vertrauensbildung & zunehmende institutionalisierung als ziel
2018 tech accord (microsoft)
2018 digital peace now (microsoft)
transparency center (kaspersky)
2018 charter of trust (siemens)
⇒ sicht wie unternehmen sich verhalten würden

initiativen aus zivilgesellschaft
2010 ICT4Peace (CH-basiert)
2013 / 2017 Talinn manuals
2017 Global Commission on the Stability of Cyberspace

effizienz normen
keine staatlichen normen bis jetzt, ideologische auseinandersetzungen
aktuellste einigung aus 2015, die vereinzelt befolgt wird
seit 2017 viele private initiativen ohne grosse koheränz
zivilgesellschaftliche initiativen mit wenig impact / jeweils starkem fokus

pros/cons bestrebungen
staatlich (+demokratisch legitimiert, +umsetzung als sicherheitsgewährleister)
unternehmen (+pushen, -private verantwortung im hintergrund)
zivilgesellschaft (+kulturwandel möglich, -nicht im fokus)

unterschiedliche ziele
staaten möchten zugriff auf daten (unlock iPhones)
firmen interessiert an kundenvertrauen, lukrativen daten
zivilgesellschaft möchte recht auf vergessen / privatsphäre

14.4 paper

must first establish norms before concrete solutions can be sought
process is as important as the end result

content
motivation why norms are useful
how such norms are formed
cyber security is not special
proposal how to proceed