Forum
InformatikerInnen für
Frieden und gesellschaftliche
Verantwortung e.V.

Ingo Ruhmann

Information Warfare: Herausforderung für politisches Gestaltungshandeln

Berlin 21.02.2015

Zur Einordnung

Info Warfare als Teil konventioneller Kriegsführung und als genuiner Kampfraum

I. Information Warfare – Akteure, Organisation, Rechtslage

- militärische
- zivile
- Rechtslage

II. Ansätze zur Begrenzung

- Rechtliche Übereinkünfte
- multilaterale internationale Abkommen
- Rüstungskontroll-Ansätze

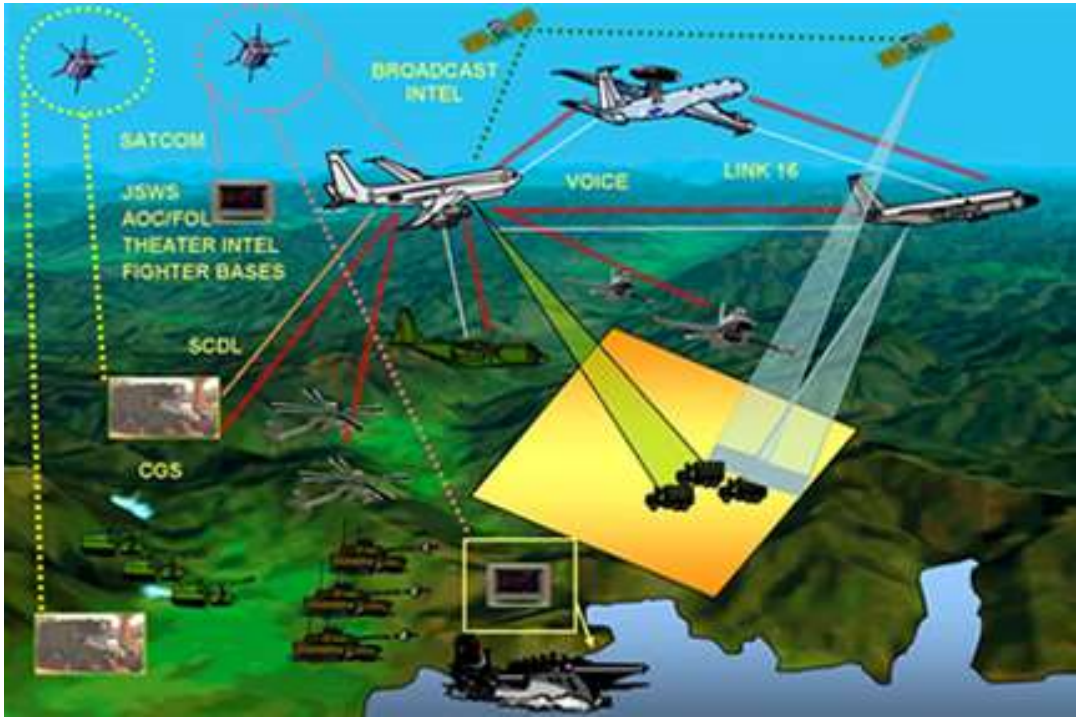
Information Warfare: Kriegführung als Steuerung vernetzter Systeme

IT-basierte Analyse / taktische Entscheidungsfindung

Auslösen militärischer Operationen

Überwachung militärischer Operationen

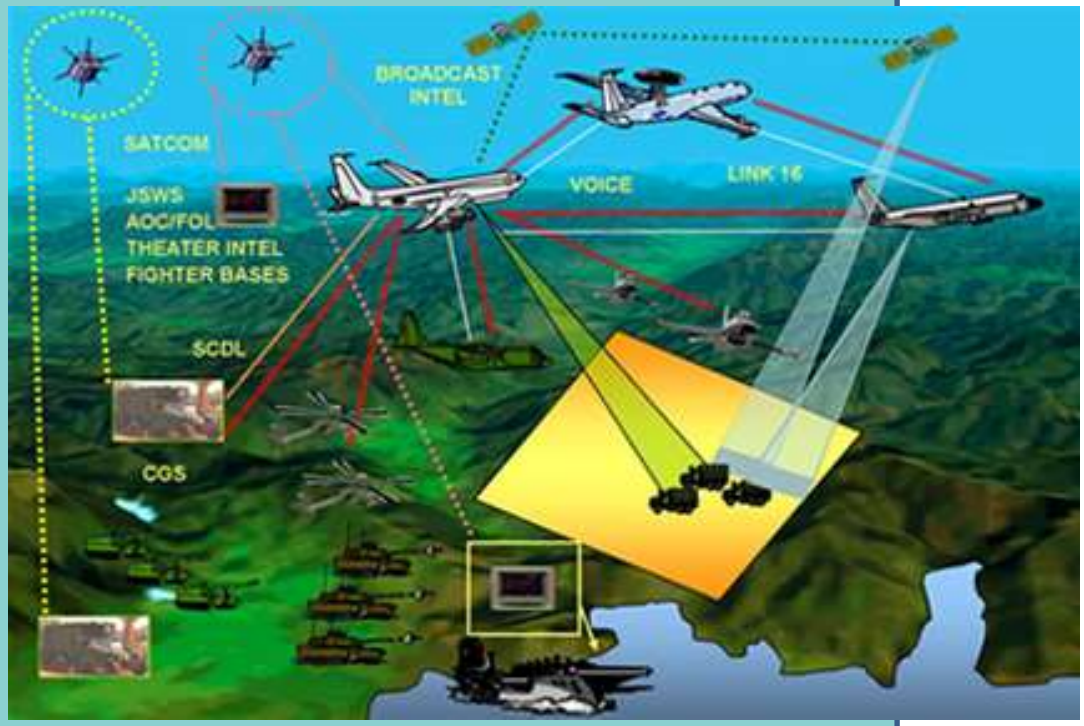
Kontinuierliche Datensammlung und -aufbereitung



Information Warfare – Ergänzung durch Kriegführung gegen vernetzte IT- Systeme

Operationsfelder des Cyber Command

IT-basierte Analyse / taktische Entscheidungsfindung



Kontinuierliche Datensammlung und -aufbereitung

Auslösen militärischer Operationen

... gegen IT-Systeme

Überwachung militärischer Operationen (konventionell + IT)

Information Warfare – Operationsfelder und Fähigkeiten

IW-Elemente	**IW-Fähigkeiten**
Electronic Warfare	Als Daueraufgabe seit WW II etabliert
Psychologische Kriegsführung	Technische Verfeinerung von Standardaufgaben der Geheimdienste und Streitkräfte
Integrierte C^4I-Infrastruktur	Ausbau seit den 60er Jahren, Integration in militärische Organisationen weit fortgeschritten
IT-gestützter Aufklärungs- und Wirkungsverbund auf dem Schlachtfeld	Seit den 60er Jahren erprobt, seit den 80ern ausgebaut. Adaption neuer Entwicklungsstufen
IT-Einsatz als Kampfmittel, **Cyberwar**	Teils zweifelhaft, teils etabliert (wenn Zugang möglich, bis zu EMP-Generatoren)
Kampf nach IW-Prinzipien	Experimentelle Erprobung (Force XXI), Erprobung einzelner Elemente in Konflikten

Information Warfare - ein deutscher Lehrberuf

Bundesministerium der Justiz

juris

Verordnung über die Laufbahn, Ausbildung und Prüfung für den gehobenen Dienst der Fernmelde- und Elektronischen Aufklärung des Bundes (LAP-gDFm/EloAufklBundV)

Nichtamtliches Inhaltsverzeichnis

LAP-gDFm/EloAufklBundV

Ausfertigungsdatum: 22.08.2006

Vollzitat:

"Verordnung über die Laufbahn, Ausbildung und Prüfung für den gehobenen Dienst der Fernmelde- und Elektronischen Aufklärung des Bundes vom 22. August 2006 (BGBl. I S. 2057), die zuletzt durch Artikel 3 Absatz 23 der Verordnung vom 12. Februar 2009 (BGBl. I S. 320) geändert worden ist"

Stand: Zuletzt geändert durch Art. 3 Abs. 23 V v. 12.2.2009 I 320

Näheres zur Standangabe finden Sie im Menü unter Hinweise

§ 14 Praxisbezogene Lehrveranstaltung

(2) In den folgenden Lehrgebieten werden Grundkenntnisse und in Teilgebieten auch vertiefende Kenntnisse vermittelt:

1. Elektronische Kampfführung,
2. Allgemeine Grundlagen der Fernmelde- und Elektronischen Aufklärung,
3. Organisation der nationalen Fernmelde- und Elektronischen Aufklärung,
4. Grundlagen und Besonderheiten im Fernmeldebetrieb
5. Grundlagen und Besonderheiten im Betrieb von Navigations-, Ortungs-, Lenk-, Leit- und Erfassungssystemen,
6. Nachrichtengewinnung und Erfassung,
7. Nachrichtenbearbeitung und Auswertung,
8. Informationsbeschaffungsmanagement des Bundes,
9. Militärische Führung und Führungssysteme in der Bundeswehr,
10. Technische Grundlagen,
11. Kommunikationssysteme und
12. Informationsaustausch und Sicherheit.

http://www.gesetze-im-internet.de/lap-gdfm_eloaufklbundv/BJNR205700006.html

Information Warfare Bw

Aufklärung, Informationsbeschaffung

Bundesnachrichtendienst (BND)

Militärischer Abschirmdienst (MAD)

Feldnachrichtenkräfte in der
Heeresaufklärungstruppe (Dietz)

Personenbefragungen, Beobachtung, 2008 **aufgelöst**

Zentrum für Nachrichtenwesen Bw (Gelsdorf)

Aufklärung, Lagebewertung aus offenen Quellen.
2007 **aufgelöst**, Teile dem BND zugeschlagen

Psychologische Kriegsführung

Zentrum Operative Information (Mayen)

Truppensender Radio Andernach, Video-Trupps, 2010 **aufgelöst** und Eingliederung in das KSA als „Gruppe Informationsoperationen“

Elektronische und Psychologische Kriegsführung, Information Warfare

Kommando Strategische Aufklärung (KSA), **(**Gelsdorf u.a.) 6.300 Militärs 700 Zivilbeschäftigte

Ab 2002: Zusammenführung der ortsfesten und mobilen Fernmelde-/Elektronischen Aufklärung (**Fm/EloAufkl**), die des Elektronischen Kampfes des Heeres (**EloKa**) sowie der Satellitengestützten Abbildenden Aufklärung (**SGA** für SAR-Lupe)

Ab 2007: Umstrukturierung, Aufgabe von Standorten heute ca. **5.500 Soldaten, 500 Zivilbeschäftigte**

Ab 2009: **Abteilung Informations- und Computernetzwerkoperationen** (Rheinbach) (zu Beginn **76 Mitarbeiter**, Der Spiegel 07.02.2009), Mai 2010 Übernahme des „Zentrums Operative Information“

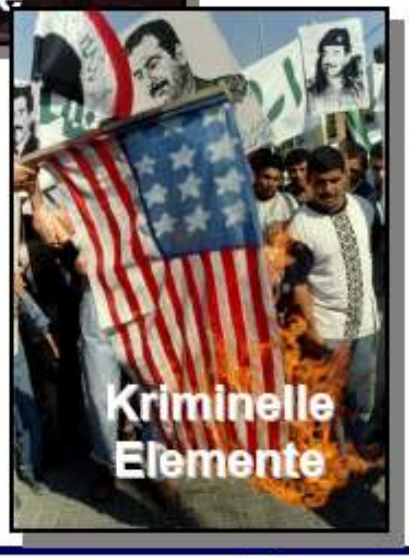
Auftrag CERTBw

24

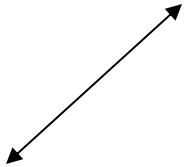
Das CERTBw ist für die zentrale Überwachung der IT-Sicherheit der Anteile im IT-System Bundeswehr (IT-SysBw), die das TCP/IP-Protokoll nutzen und nicht in der Betriebs-verantwortung der BWI IT liegen, verantwortlich.

Nationale Zusammenarbeit CERTBw

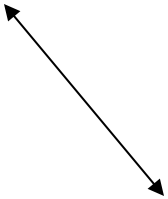
Wer bedroht uns eigentlich?



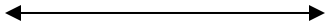
KSA
FmEloAufkl, EloKa,
Cyber Warfare



?



CERT-Bw
Schutz der Bw-Netze



BSI
Abwehr von Angriffen auf staatliche Stellen, Informationssammelstelle

IW – Operationen und Fähigkeiten Deutschlands

IW-Elemente	**IW-Fähigkeiten in Deutschland**
Electronic Warfare	**KSA**
Psychologische Kriegsführung	**Zentrum Operative Information / KSA**
Integrierte C^4I-Infrastruktur	Lückenhafte Integration diverser Systeme, HERKULES-Aufgabe
IT-gestützter Aufklärungs- und Wirkungsverbund auf dem Schlachtfeld	Taktisch-operativ in kleinen Kampfgruppen. System- und Medienbrüche bei Vernetzung verschiedener Einheiten
IT-Einsatz als Kampfmittel	Überwiegend zweifelhaft - **KSA**
Kampf nach IW-Prinzipien	Anbindung an Kampftruppe unklar; KSA-Abteilung **Informations- und Computernetzwerkoperationen**

Schutz der Infrastruktur **CERT-Bw – 2012 ca. 40 Mitarbeiter**

http://www.baain.de/portal/a/baain/!ut/p/c4/LYrBCsIwEAX_aDdNvOjNUgQPXgTRetu2oSxuNyVs9eLHm4BvYC7z8IkFpTfPZJyUBB_Yj3wYPjAQsQK9bIsiQCJRCe_1P0UYk0artqjGxXMmSxnWlE1q2XIuBXjC3jVd63xw_zXfvb-cbmEXfHdur7guy_EH_xn13g!!/

Cyberwar rechtlich

*Computermanipulationen im engeren Sinne (seit **1986**)*

- Ausspähung von Daten (202aStGB)
- Computerbetrug (§263a StGB)
- Fälschung technischer Aufzeichnungen (§268 StGB)
- Fälschung beweiserheblicher Daten (§269 StGB)
- Datenveränderung (§303a StGB)
- Computersabotage (§ 303b StGB)
- Bruch des Fernmeldegeheimnisses (§206 StGB)

Zusätzlich in Betracht kommende Straftatbestände

- Herbeiführung einer Explosion durch Kernenergie, Freisetzung ionisierender Strahlung, Vorbereitungsdelikte (§310b ff StGB),
- Störung von Fernmeldeanlagen (§317 StGB)
- ...

Computerstraftaten lassen sich *als Terrorismusdelikt* nach §129a StGB werten bei Angriffen auf IT-Systeme, sofern es sich um gemeingefährliche Straftaten handelt nach

- §305a StGB - Zerstörung wichtiger Arbeitsmittel
- §315 StGB - Gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr
- §316b StGB - Störung öffentlicher Betriebe (Bahn, Post, Versorgung mit Wasser, Licht, Wärme, Kraft)

Keine Rechtsgrundlage für wesentliche Werkzeuge der IT-Sicherheit

- Das TMG untersagt die Protokollierung von vollständigen IP-Nummern
  - a) über die konkrete Nutzung hinaus
  - b) in vollständiger Form (nicht-pseudonymisiert)
  - c) ohne Einwilligung des Nutzers (= Angreifers)
- Rechtlich ist die Speicherung von IP-Nummern und deren Nutzung bei der Analyse des Datenverkehrs zu Sicherheitszwecken nur für die Sicherheit der IT des Bundes erlaubt (§5 BSIG)
- Weder BKA noch BND, CERTs oder sonst wer darf Protokolldaten sammeln

➔ **Haben Sie schon wegen eines Computerschädlings eine Strafanzeige versucht? Wie wollen Sie das auch beweisen?**

Rechtslage und NATO-Rechtsauffassung zu Computermanipulationen

Cyber Warfare

Der Einsatz militärischer Gewalt kann gegen einen Cyber-Angreifer, der Schäden an Leib und Leben verursacht, zulässig sein

Regeln 14,15 des „Tallinn Manual on the International Law Applicable to Cyber Warfare“, S. 61ff

http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Flight%2Flayout.xml&showFlipBtn=true

Computerkriminalität

Cybercrime-Konvention

Artikel 23 – Allgemeine Grundsätze der internationalen Zusammenarbeit

„Die Vertragsparteien arbeiten untereinander im Einklang mit diesem Kapitel im größtmöglichen Umfang zusammen...

Artikel 25 – Allgemeine Grundsätze der Rechtshilfe

1 Die Vertragsparteien leisten einander im größtmöglichen Umfang Rechtshilfe für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat.

http://conventions.coe.int/treaty/ger/treaties/html/185.htm

Sollen Cybermanipulationen mit „physischer Gewalt“ militärisch unterbunden werden, weil die Rechtshilfe unbefriedigend gelöst ist oder, bei Spionage keine Kooperation zu erwarten ist?

Ressourcen ziviler Akteure bei Cyber Warfare (weit gefasst)

Polizei / LKA Lt GdP: Ca **360 MA**

LfV / BfV K.A. zu Mitarbeitern

		1986		**1989:**		**1991:**	
BND	->	ZfCh	->	ZSI	->	**BSI**	**550 MA**

IT-Lagezentrum (BSI): „täglich 24 Stunden mit 1 Fachkraft in Bereitschaft“

<u>Inhaltsbeobachtung</u>: GTAZ, GIZ

GTAZ: **198** MA des Bundes, **31** der Länder Bt.-Drs. 16/10007

GIZ: **51** MA Drs. 17/5557

<u>Lagebeobachtung zu Cybersicherheit</u>

Cyber-Abwehrzentrum: **10** MA

Drs. 17/5694

Nationales Cyber-Abwehrzentrum

CERTs (ca**. 15** im CERT-Verbund)

<u>Ressourcen</u>

IT-Sicherheits-forschung

Defensiv: **30 Mio. p.a.**

BND-Aufstockung

Offensiv: **300 Mio.**

<u>Personal</u>

Inhaltsbeobachtung: 280 + B/LfV

Ermittlung, Cyberlage: **920**

zivile Einrichtungen ohne Dopplungen: ca. 900

Mit CERTBw 940

KSA 6.000

Fazit

1. Unzureichende staatliche Gefahrenvorsorge

- Fachexpertise ist stärker bei kommerziellen IT-Sicherheitsfirmen. Zivile Behörden der IT-Sicherheit und der Strafverfolgung verfügen nicht über angemessene Ressourcen; Militärs sind weder kompetenter noch besser ausgerüstet. Es fehlen rudimentäre zivile rechtliche Grundlagen.
- Defizite bestehen teilweise >15 Jahre.
- Mängel in der zivilen IT-Sicherheit und der internationalen Kooperation lassen sich nicht kompensieren durch militärische Maßnahmen – d.h. zwischenstaatliche Selbstjustiz.

2. Forschung und Technik

- Defizite bei technischen Analysewerkzeugen beseitigen, Verbesserung der IT-Sicherheit: mehr Fachleute, auch mehr Forschungsförderung.

3. Politische Gestaltung

- Erfordernisse und technische Möglichkeiten einer Cyber-Rüstungskontrolle sind nicht ansatzweise analysiert oder realisiert. Politische Gestaltungsideen fehlen zu sicherheitspolitischer Cyber-Stabilität und zivilen Lösungen.

II. Ansätze zur Begrenzung

- Rechtliche Übereinkünfte
- multilaterale internationale Abkommen
- Rüstungskontroll-Ansätze

Info War und Rüstungskontrolle: USA und Russland

USA

1998: erste akademische Studien zu InfoWar
Lawrence T. Greenberg et.al.: Information Warfare and International Law, Defense University Press, http://www.dodccrp.org/files/Greenberg_Law.pdf

2001 und 2007 Kongress-Reports zu Cyberwar und Rechtsfragen

2009 Gespräche USA-Rußland zu „Verbesserung der Internet Sicherheit und Begrenzung der militärischen Nutzung des Internets“

2011 International Strategy for Cyberspace

Russland

International code of conduct for information security

Annex to the letter dated **12 September 2011** from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the UN Secretary-General (A/66/359):

•“Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression,”

•“To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks”

Gemeinsames Expertenpapier 2011 :

•Entkopplung kritischer Infrastrukturen von anderen Netzen

•Markierungen für konventionskonform geschützte IT-Systeme

•Analyse der Technik: gibt es Eigenschaften analog zu unerlaubten Waffen nach dem Genfer Protokoll

• ‘other-than-war-mode’ zur Klärung der Anwendbarkeit von Konventionen

Aktivitäten zu Info War und Rüstungskontrolle in Deutschland

1994/95 Der Deutsche Bundestag betrachtet Konsequenzen des militärischen IT-Einsatzes für Sicherheitspolitik und Rüstungskontrolle.

Beauftragung einer systematischen Studie zum IT-Einsatz in der Kriegsführung und den Konsequenzen für Rüstung und Rüstungskontrolle durch das Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB)

> Ralf Klischewski, Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie; Gutachten des FIfF für das Büro für Technikfolgenabschätzung des Deutschen Bundestages, Bonn, März, 1995

Auswärtiges Amt, Referat 241:
„... Vertrauens- und Sicherheitsbildende Maßnahmen bezüglich Cyber-Sicherheit."
2007/08: AA richtet **Cyber-Koordinierungsstab** ein und besetzt Posten mit Cyber-Beauftragten an deutschen Auslandsvertretungen. Der Koordinierungsstab erarbeitet entsprechend der neuen Cyber-Sicherheitsstrategie die deutsche Position für internationale Gremien.

Dual Use: Beispiele und Erfahrungen im Technologiebereich

Exportkontrolle

CoCom: „Coordinating Committee on Multilateral Export Controls“

Nachfolge 1996: **Wassenaar Agreement**

33 Mitglieder: NATO-Staaten, Verbündete (Japan, Kanada, Australien, etc.), Russland, Südkorea, Südafrika etc.

Aufgabe:

- Erstellung von Technologielisten, Definition von dual-use-Gütern
- Überwachung: BAFA
- Umfasst auch Alltagstechnik (RADEON-Grafikkarten)

Beispiele und Erfahrungen im Technologiebereich

U.S. Export Administration Act

1983 zeitweises Versagen des Exports von UNIX-Software aus den USA an Deutschland wegen enthaltener Krypto-Software:

> "Das U.S. Department of Commerce verhängte ein temporäres Embargo über die gesamte UNIX Software, sodass es unglücklicherweise zu einer Verzögerung kommen wird"

AT&T an Uni Dortmund, 1983

Wassenaar

- Kryptoprodukte sind weiter dual-use-Güter
- Keine Exportkontrolle für Krypto-Produkte unter 56 Bit Schlüssellänge.
- Erweiterung der Exportkontrolle auf starke Kryptographie über 64 Bit, "die für den Massenmarkt bestimmt ist".

2. Juni 1999 Kabinettsbeschluss zu liberalen Krypto-Eckwerten - Teil einer autonomen Linie Deutschlands

Wassenaar Dezember 2013

Aufnahme von Trojaner-Software in Dual-Use-Liste

Entwicklungen und Anwendungen von Informationstechnologien, die friedenswissenschaftliche Aufmerksamkeit verlangen

1) **Infowar**: Militärische Machtprojektion (Präzisionswaffen, Drohnen), Destabilisierungstendenzen

- IT-Einsatz als **Wehrkraftverstärker** („Force Multiplier“) und Motor militärischer Konfliktlösung für große Militärorganisationen
- IT-Einsatz stärkt auch kleine militärische Organisationen mit mäßiger Technikaffinität und wenigen technischen Möglichkeiten

2) Hohe **Intensität** sowohl herkömmlicher militärischer Aktionen als auch bei Cyberangriffen (Infowar und Cyberwar)

3) Cyberwar: Erosion der Zivilgesellschaft, dauerhafte und umfassende Datensammlung

4) Ausweitung von „**non-wars**“, geheimdienstlicher Aktivitäten und jeder anderen Form unkontrollierbarer zwischenstaatlicher Aggression

Politische Schlussfolgerungen für die Friedensforschung

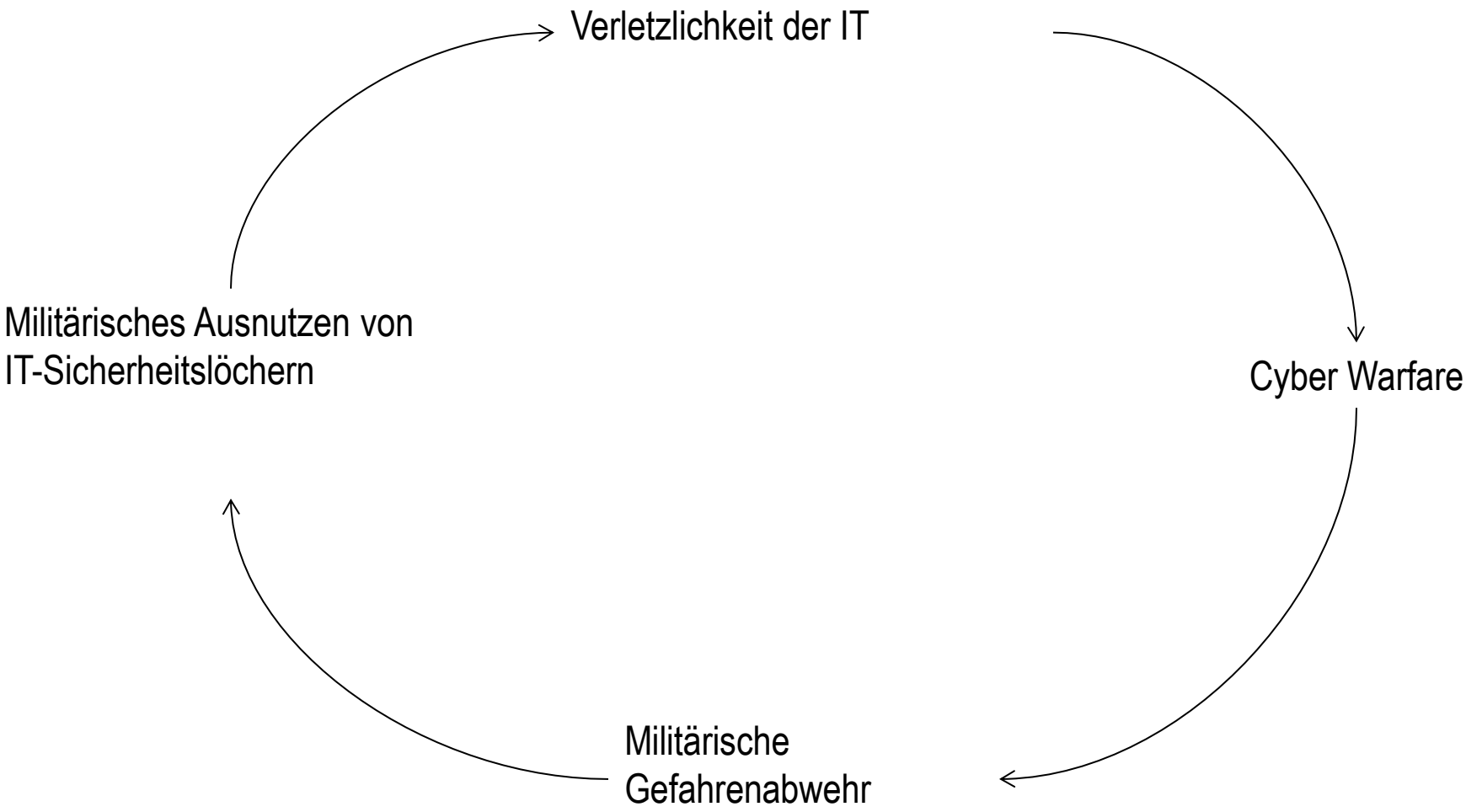
- **Info Warfare** wird seit 20 Jahren ausgetragen. Die Art der Präzisionswaffen und ihr Einsatz haben sich geändert, aber weder militärischer Anspruch an global ausgeführte Schläge und die Doktrin noch die Kritik daran.
- „**Cyberwar is Coming**“ (Arquilla/Ronfeld 1993) ….. **for 20 years now**! Die aktuelle Cyberwar-Debatte ist der dritte Aufguss derselben Inhalte.
- **IT-Sicherheitsdefizite -** weit größer als Cyberwar-Aktivitäten. Beides zu vermischen, lässt keine Lösungsperspektive zu. Bessere IT-Sicherheitstechnik, mehr Fachkompetenz bei Unternehmen und staatlichen Stellen machten vieles an dieser Debatte überflüssig.

Raus aus der Defensive!

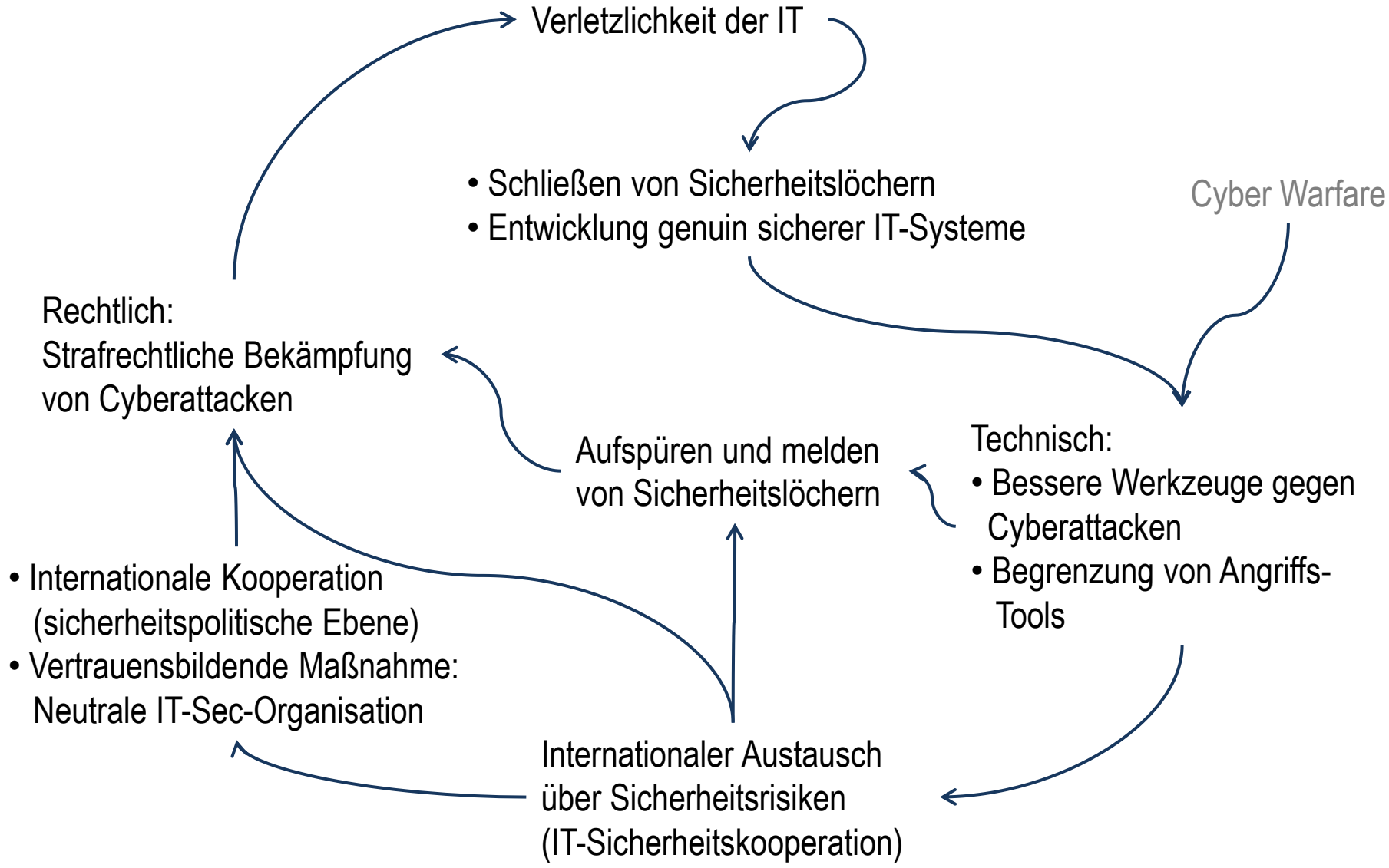
- **Koalitionspartner:** IT-Sicherheitsfirmen und zivile Internet-Verantwortliche (RIPE, IETF etc.), BAFA, BSI, Polizei etc. suchen umsetzbare Lösungen - Geheimdienste dagegen neue Arbeitsfelder. Die Friedensforschung könnte viele Kooperationspartner gewinnen. Nötig sind dafür neue Ideen (IT-Sicherheit ebenso wie sicherheitspolitisch) und Partner weltweit.
- Nötig ist en **ziviles, technisches und sicherheitspolitisches Agenda-Setting**.

Umsetzungsansatz: Cyberpeace-Kampagne des FIfF

Politische Folgen: Der IT-Unsicherheitszyklus



Dem IT-Unsicherheitszyklus entgegen wirken



Dem IT-Unsicherheitszyklus entgegen wirken

Rechtlich

- national: IT-Sicherheitsgesetzgebung,
- international: Abkommen zur zivilen Kooperation

Sicherheitspolitisch

- Ächtung von „D-Waffen“, „Erstschlagverbot“,
- Exportkontroll-Regelungen, Rüstungskontroll-Abkommen, Überwachung der Regeln mit internationaler Einrichtung,
- Begrenzung von Ausspähung und Kompromittierung von IT-Systemen

Technisch

- Bestandsaufnahme der Kompromittierung,
- Ressourcen für intensive Entwicklung von IT-Sicherheit (Systeme und Werkzeuge),
- Ausbau von IT-Sicherheitszentren (CERTs u.ä.) ,
- verstärkte Auditierung ausgewählter Bereiche (Infrastrukturen)