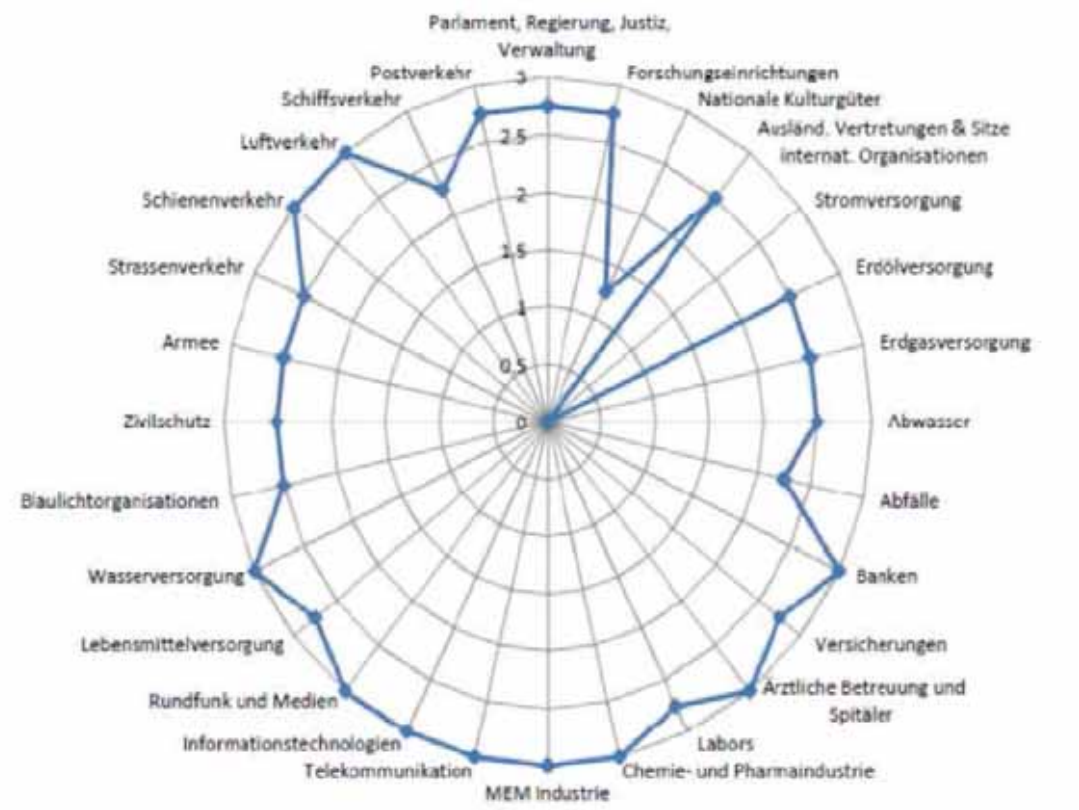
Sicherheit von kritischen Infrastrukturen in der zunehmend digital vernetzten Welt

Andy Mühlheim, 2016

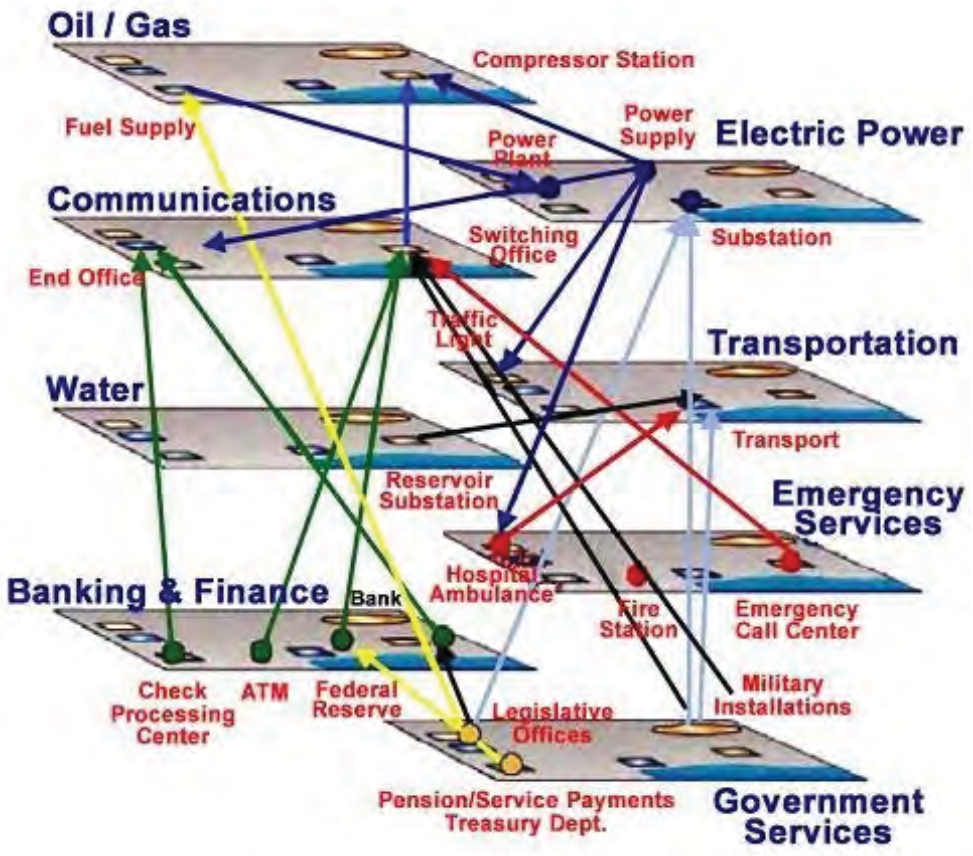
Was ist eine kritische Infrastruktur?



Abhängigkeiten der Energieversorgung (BABS)

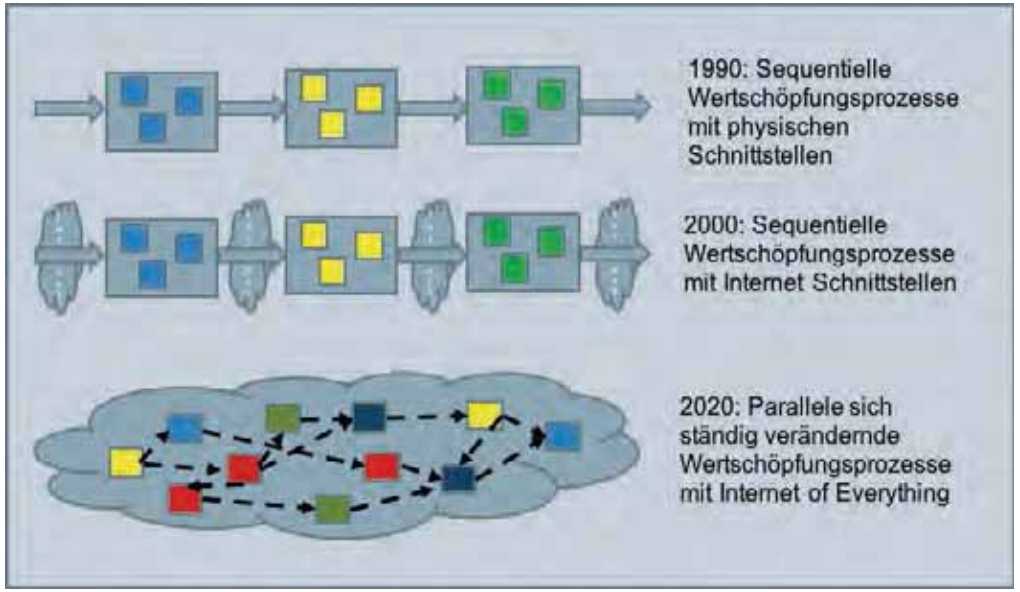
- **Hohe volkswirtschaftlichen Risiken**
- **Keine Substituierung möglich**
- **Hohe Abhängigkeiten vorhanden**

Ungesehene und ungewollte Nebenwirkungen als neue Bedrohung der vernetzten Welt



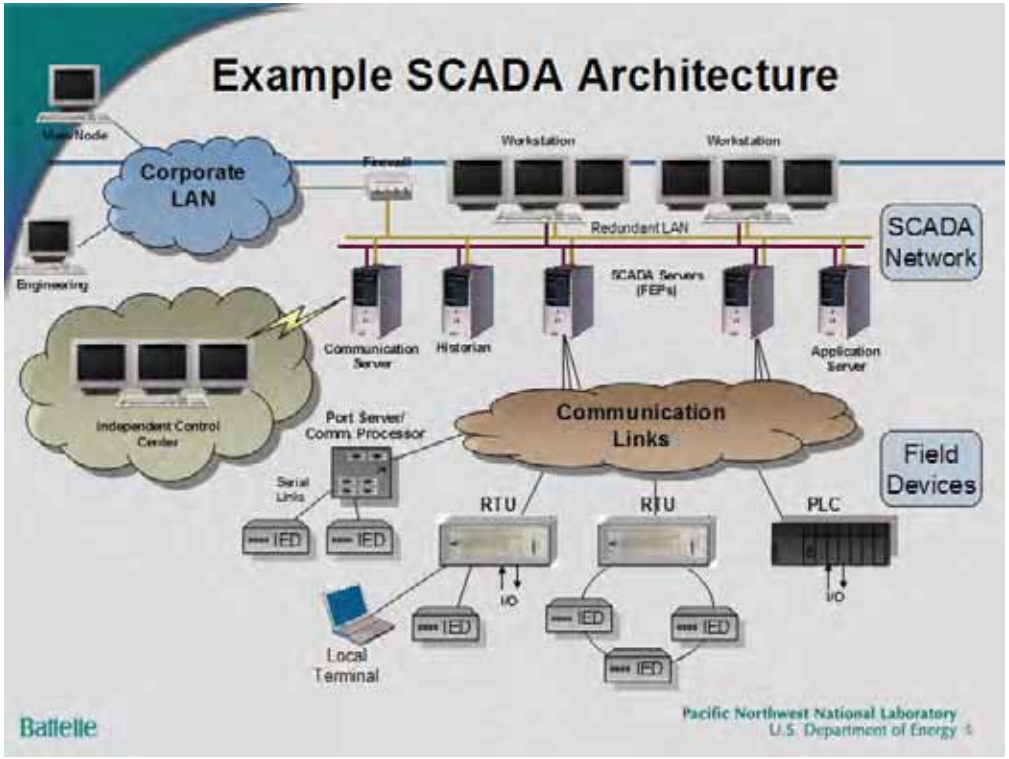
- **Hohe Komplexität**
- **Ungenügendes Verständnis der Abhängigkeiten**
- **Risikoplanung nur auf losgelöste und isolierte Ereignisse**

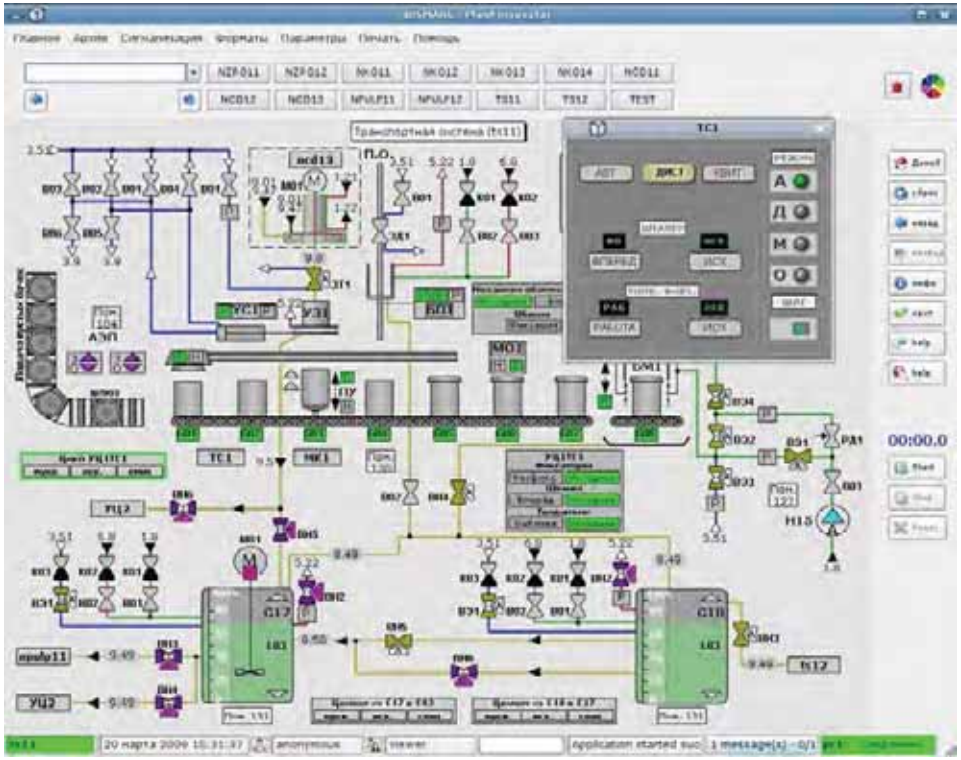
Industrie 4.0 konvergiert IT mit OT



	Information Technology	Operational Technology	Operational Technology for KI
Systemaufbau	Transaktionsbasiert	Real-time	Real-time
Zeitkritikalität	Vernachlässigbar	Kritisch	Kritisch
Verfügbarkeit	Normal (Back Office)	Sehr hoch Prozesskritisch	**Unterbruchsfrei Systemkritisch**
Risikoträger	Primär unternehmerische Risiken	Primär unternehmerische Risiken	**Primär volkswirtschaftliche Risiken**

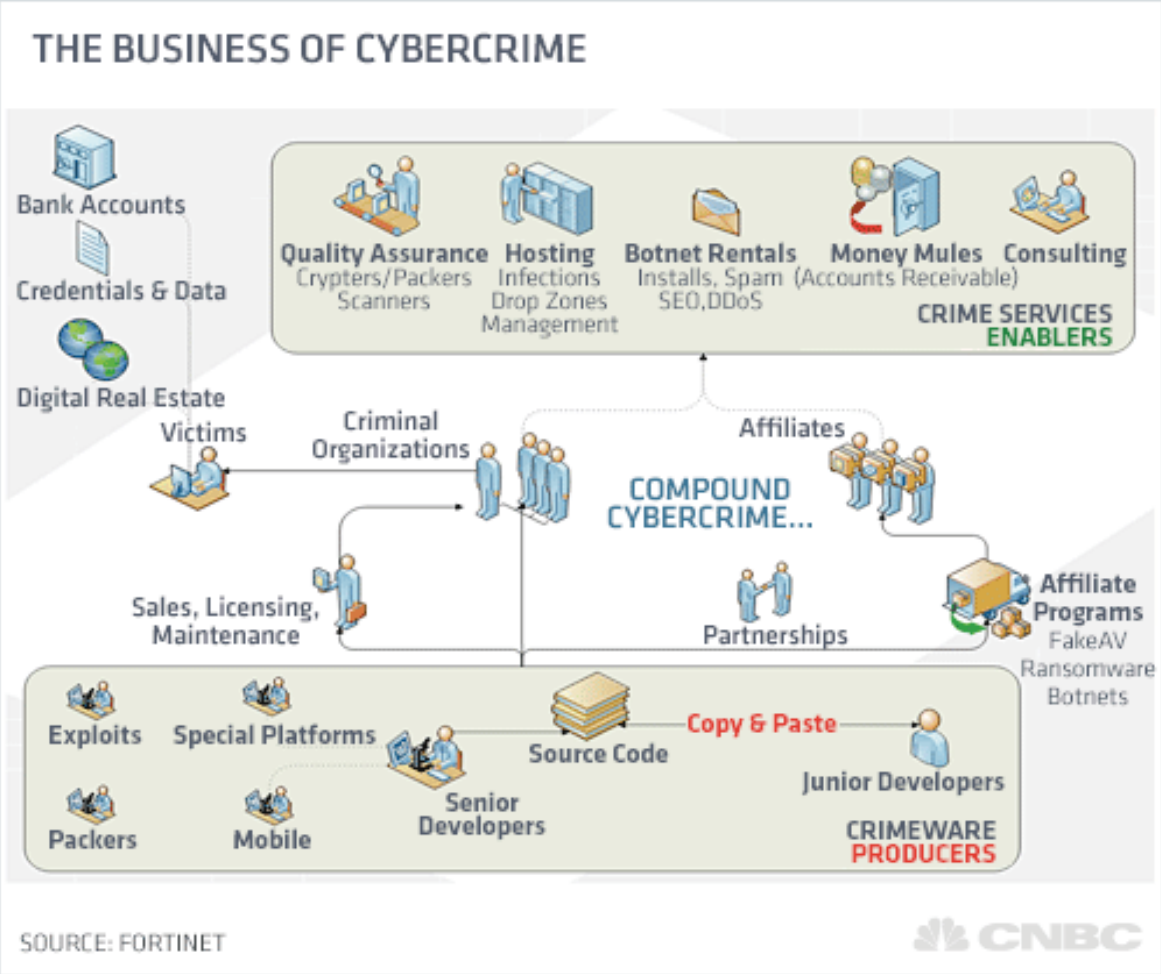
Operational Technologien sind Einzelentwicklungen





- **Lange Innovationszyklen**
- **Systemaktualisierungen und Patching nur bedingt** möglich
- **Security-Tests nur beschränkt** möglich
- **Remote Zugänge** für Dritte schwer handbar
- **Hoher individueller Entwicklungsanteil**

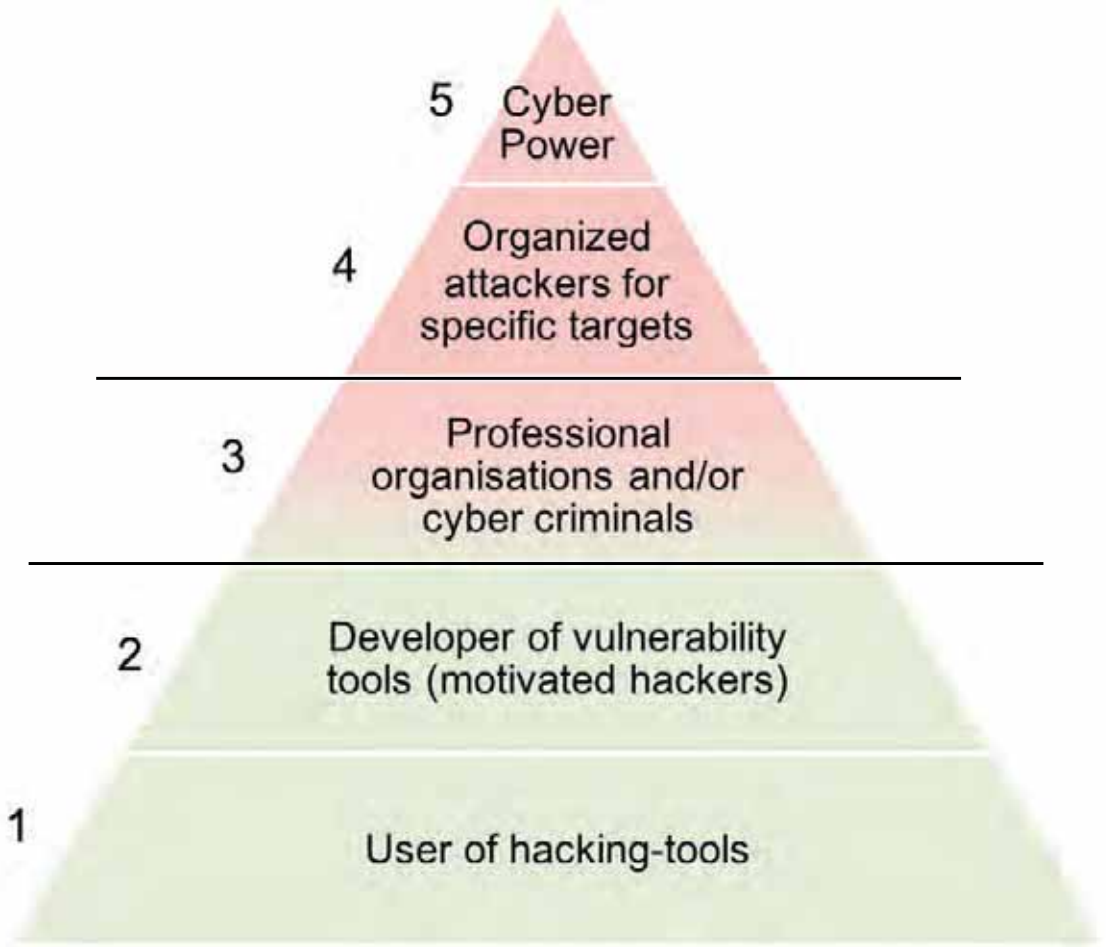
Cyber Angriff „as a Service“



= 100 CHF

= Schaden von 1 Mio CHF

Die Cyber Threat Pyramide für kritische Infrastrukturen



- **Absicht**
- Qualifizierte Bedrohungen
- Unbekannte Formen

- **Absicht**
- Qualifizierte Bedrohungen
- Bekannte Formen

- **Zufällig**
- Unqualifizierte Bedrohungen
- Bekannte Formen

Cyber Defense Dissymetrie

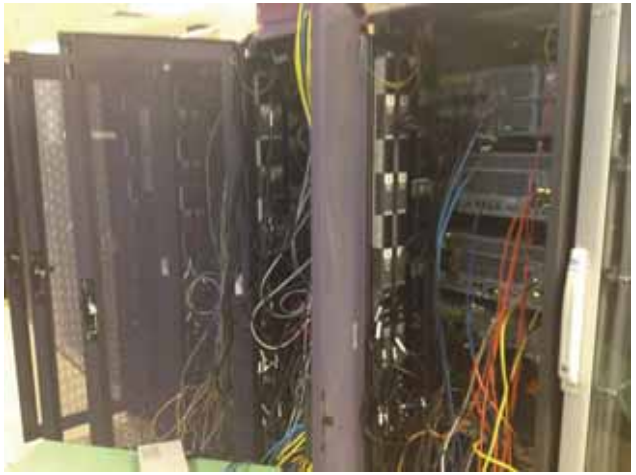
V: Muss alle Löcher stopfen
A: Braucht ein einziges Loch

V: Ist abhängig von Dritten
A: Nutzt Dritte

V: Arbeitet zu normalen Arbeitszeiten
A: Arbeitet ausserhalb Arbeitszeiten

V: Macht seinen Job
A: Besitzt eine Passion

KI Herausforderungen



Über die Jahre gewachsene Systeme

Isolierte Betrachtung von Risiken

Breiter Widerstand gegen steigende Strompreise

Keine Akzeptanz gegenüber Kosten

Computer: Indien will 500 000 IT-Experten gegen Cyberattacken ...
ZEIT ONLINE - 16.10.2012
Neu Delhi (dpa) - Indiens Regierung will zusammen mit privaten ... da die Cyber-Kriminalität mittlerweile zu den größten Bedrohungen der ...

Power systems easy target for cyber criminals

US-Verteidigungsminister zeigt sich für Cyberwar-Erstschlag bereit
Heise Newsticker - 12.10.2012
Die USA sind in der Lage, Bedrohungen aus dem Cyberspace mit einem Erstschlag zu begegnen. Das sagte US-Verteidigungsminister Leon ...

Indien kämpft gegen Cyber-Attacken | tagesschau.de
21. Aug. 2012 - Die Regierung in Neu-Delhi spricht von Cyber-Terror und versucht sich zu wehren. Bislang wurden 200 ... News in English - Haberler ... Massenaufauf am Bahnhof in Bangalore, der indischen Computer-Stadt. Tausende ...

'Massive' cyber attacks target Middle East oil companies
... Middle Eastern oil and gas companies have been targeted in massive attacks on their computer networks in an increasingly open cyber war where a new virus was discovered just this past week.

Cyberspace is battlefront of the future: US defense secy
... Cyberspace is the battlefield of the future, with attackers already going after banks and other financial institutions and developing the ability to strike US power grids and government systems.

New version of Flame virus discovered: Researchers
... A new cyberespionage tool linked to the Flame virus has been infecting computers in Lebanon, Iran and elsewhere, security researchers said.

US facing possibility of 'cyber-Pearl Harbor', pre-emptive action possible: Leon Panetta

Japan vulnerable to cyber-attack
... When most of the world was watching the Olympic Games, dozens of Japanese students were enthralled by the world of computer viruses and bugs.

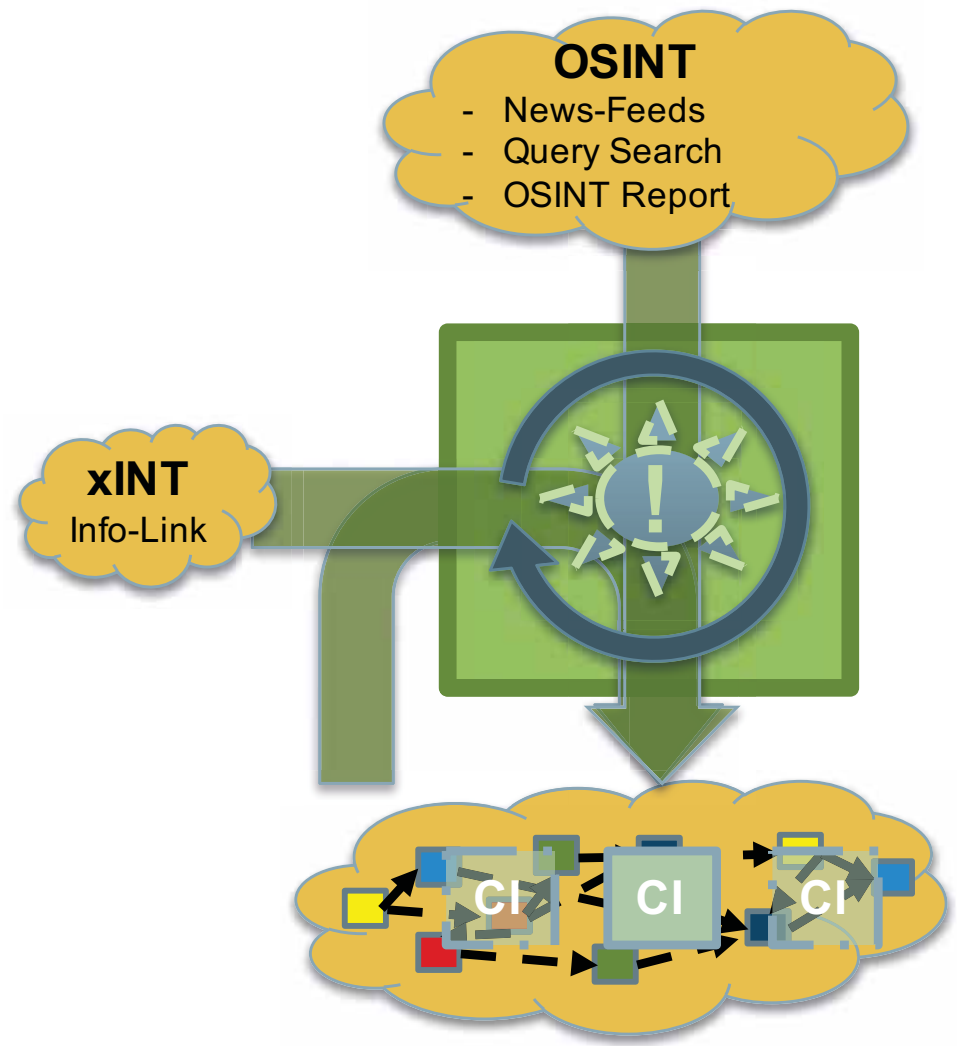
Die Cyber-Spirale dreht sich bereits

Das volkswirtschaftliche Paradox

Volkswirtschaftliche Risiken

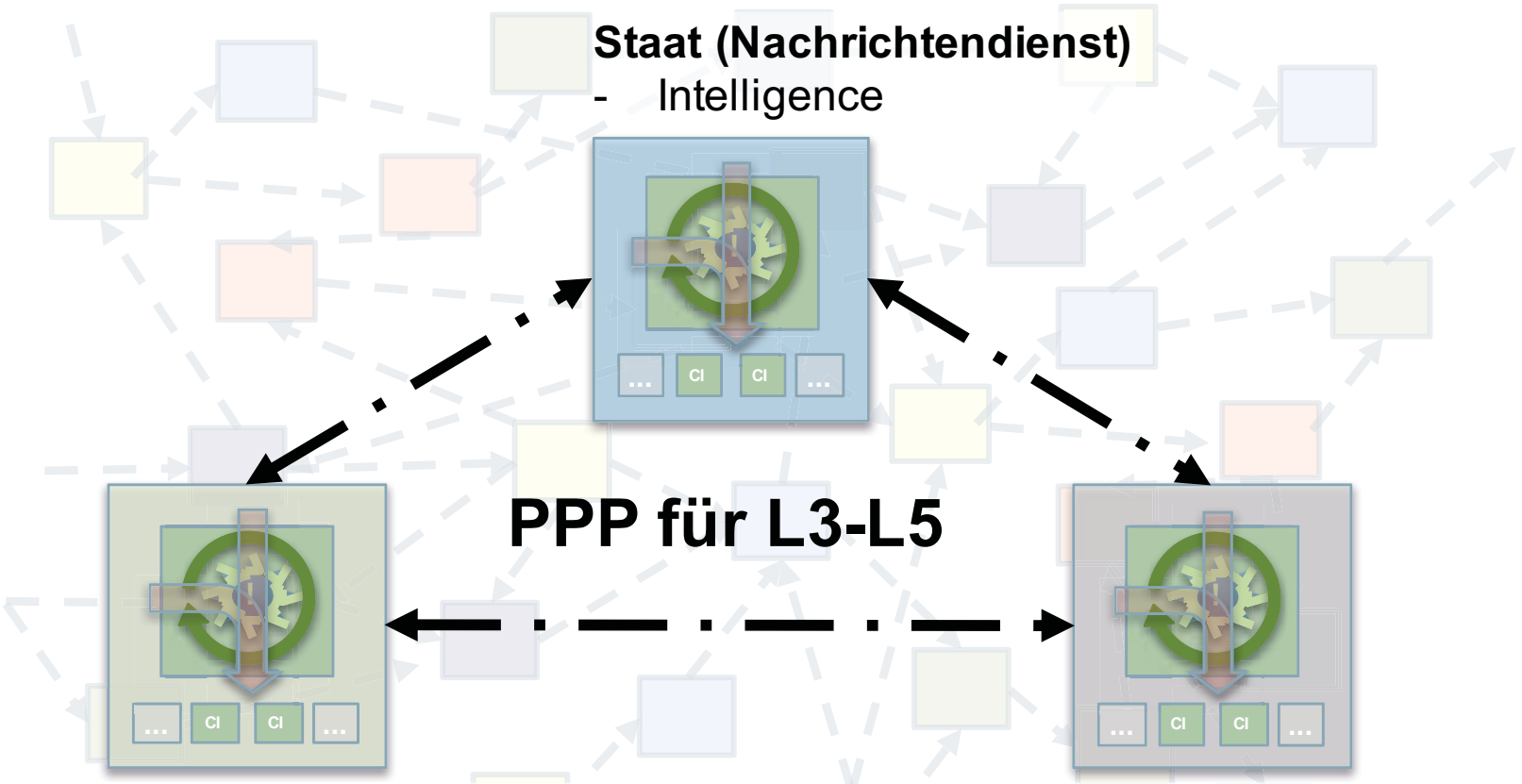
Betriebswirtschaftliche Unternehmensführung

Ein Cyber Alert Network für Kritische Infrastrukturen



- **Verstehen der kritischen Prozesse, Abhängigkeiten, Bedrohungen und Absichten**
- **Gegenseitige Unterstützung**

Cyber Defense: PPP - Ein Netzwerk aus Wirtschaft, Armee und Staat, Hand in Hand



Armee
- Subsidiäre Unterstützung
- Verteidigung

Industrie
- Grundschutz
- Eigenverantwortung
- L1, L2 und L3

Cyber Defense ist:

Ein **Netzwerk** welches ein **Netzwerk** vor einem **Netzwerk** schützt