SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Mitglied der
Akademien der Wissenschaften Schweiz

SATW TPF ICT Security & TPF Cloud:

Sichere ICT und Cloud aus der Schweiz: Fiktion oder Realität?

Anschliessend Panel

Sichere ICT und Cloud aus der Schweiz: Standort und die Rolle der Wissenschaft

Bernhard M. Hämmerli

Inhalt

- Ergebnis 1. SATW Debatte 2. April 2014 an der ETHZ

- ICT & Cyber-Bedrohungslage bis 2014 mit Schlussfolgerungen
- Update ICT & Cyber-Bedrohungslage 2015 mit Schlussfolgerungen
- Handlungsbedarf Schweiz im Bereich Cyber-Security

- Aufbau unserer Veranstaltung

SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Ergebnisse 1. SATW Debatte

2. April 2014 an der ETHZ

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Bedrohungslage: Paradigmawechsel

Snowden ➔ Referenzen für Expertenwissen: war eigentlich bisher bekannt, aber man konnte die Experten als Verschwörungstheoretiker hinstellen.

- Spitzendiplomatin US Victoria Nuland, am 7.2.14 erstaunt über die Sprachqualität des russischen Abhörens "Fuck the EU"

- "**If a nation-state wants to hack you, they will succeed to do so**"
  (Bruce Schneier 2013)
  Die politische Kontrolle über die Verwendung der Resultate ist abhängig vom Staat

- Internet war und wird immer ein "öffentlicher" Raum bleiben!
  ➔ Lassen Sie sich nicht vom Internet abhalten aber sein Sie bewusst was Sie tun!
  - Datensparsamkeit (nur wenn zwingender Grund Daten im Computer),
  - Uminterpretation des Kontextes (Bsp. Gelichberechtigung),
  - Negative Campaign (Anlassbezogene Datenauswertung, (Bsp. Sport-Risikoverhalten))

Analyse der technischen Möglichkeiten auf den nächsten Slides

Combined Stealth Attack Architecture

- Multiple pieces of code makes little or no meaning, but together they make up the malicious code.

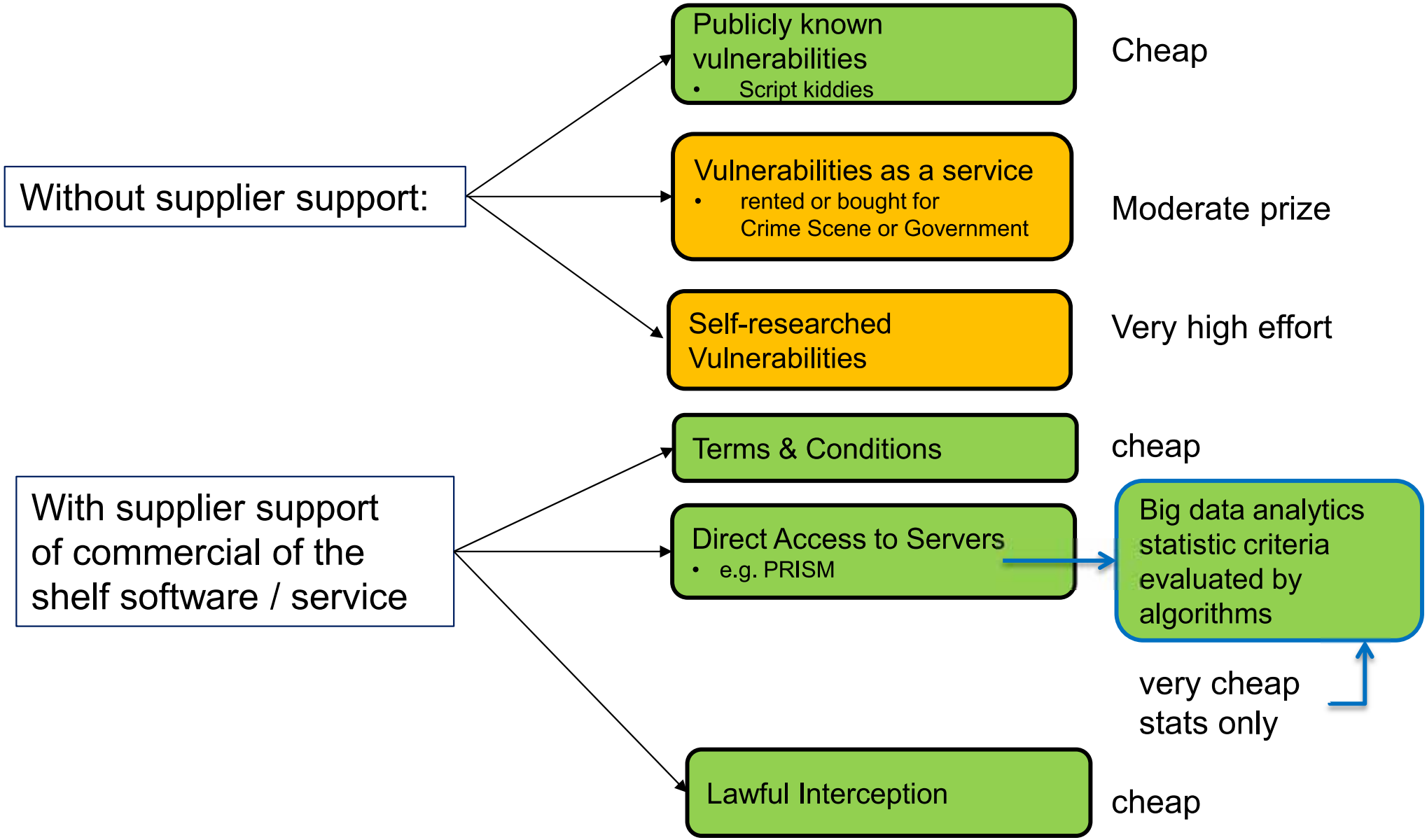
- Can be distributed in two or more of the following ways:
  - Operating system software
  - Be a part of popular applications or an additional application
  - Added in development process
  - Added into hardware or added as extra hardware
  - Sent through updates from trusted vendors*
  - …

*Requires either to “collaborate with” or “hack” a vendor, or ”inject an undercover employee”.

➔ Combination makes the attack almost impossible to detect ...
Ideal: stealth & untraceable, immune to malware detection: see appendix A1

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Technical options for attacks
Blue Eye Version:
What we want to see

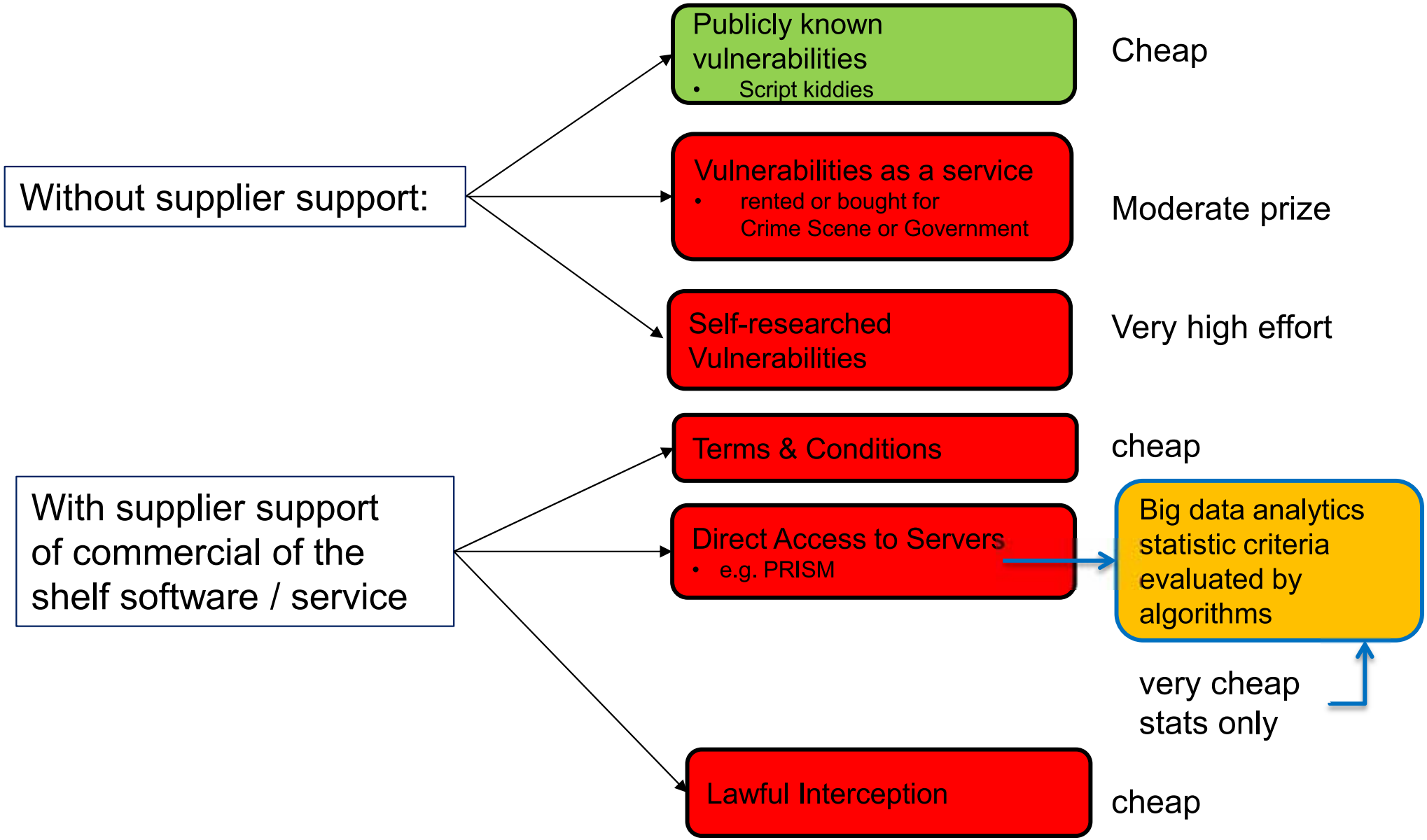


SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Technical options for attacks

Realistic Version today:

What we hate to see



Electricity Grid in U.S. Penetrated By Spies

By SIOBHAN GORMAN

Updated April 8, 2009 11:59 p.m. ET

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks. *Associated Press*

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

Wall Street Journal: http://online.wsj.com/news/articles/SB123914805204099085

Off-Schalter in China für US Stromversorgung?

1. ICT & Cyber-Bedrohungslage bis Ende 2014 mit Schlussfolgerungen

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

2014 Grundlegende Änderungen

Ab 2013: Die Intention dass Nordkorea eine Armee von 6000 Cyber-Soldaten aufbaut.
6.1.2015 Bestätigung in FAZ.

ICT Delegationsreise Parlament nach Shenzhen

John Suffolk, früherer CIO und UK und heute
Global Security Officer bei Huawei:

«For 100 USD you can download a Software to hack any system!»

Weshalb trotzdem Sicherheit machen?
➔ Die Zahl der Personen, die angreifen kann, wird kleiner.

Schlussfolgerung: Heute ist man auf das «gute Verhalten» von jedem Internetnutzer angewiesen. Das Budget für Angriffe ist klein, dasjenige für den Schutz unmöglich hoch.

SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Was bedeutet Cyber Operation?

2014 Grundlegende Änderungen

20. November 2014: Cyber-Abschreckung als entscheidende Strategie!

Michael Rogers, Chief Admiral, NSA-Direktor und Leiter US Cyber Command sagt, dass ihm die reine Verteidigung im Cyberspace wie eine Verlierer-Strategie vorkommt. Man müsse definieren, wie man offensiv vorgehen könnte.
Im Original: “We need to define what would be offensive, what would be an act of war,” he said. “**Being totally on the defensive is a very losing strategy to me**.”

24. November 2014: Unternehmen werden Angegriffen und erpresst

75% der Server des Unternehmens Sony wurden lahmgelegt. Die Rückverfolgung der Angreifer war schwierig. Bevor eine forensische Gewissheit gefunden werden konnte, wurde „Profiteur“ Nord-Korea für diese Aktion verantwortlich gemacht.

http://deadline.com ; http://www.wsj.com
http://www.computerweekly.com/news/2240237500/North-Korea-slams-hostile-US-sanctions-over-Sony-cyber-attack?asrc=EM_EDA_38336197&utm_medium=EM&utm_source=EDA&utm_campaign=20150105_North%20Korea%20slams%20'hostile'%20US%20sanctions%20over%20Sony%20cyber%20attack_
http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/nordkorea-stockt-hacker-truppe-auf-6000-soldaten-auf-13356205.html

Diktator Kim Jong-un befehligt mittlerweile 6000 Hacker in seiner Sondereinheit „Büro 121“. Doppelt so viele wie bisher angenommen!

Die neuen Zahlen stammen aus einer Analyse des südkoreanischen Verteidigungsministeriums.

Norwegen fühlt sich mit 1000 Cybersoldaten schwach und deshalb Unwohl: hat auch eine gemeinsame Grenze mit Russland

Sony Attack: 24. November 2014

Sony attack (Nord Korea): The attack also resulted in the **destruction of about three-quarters of the computers and servers** at Sony firm's main operations, according to a weekend report in the New York Times.

- Data released online showed that the attackers accessed a wide variety of data, including a list of employee salaries and bonuses; social security numbers and dates of birth; employee performance reviews; criminal background checks and termination records; correspondence about employee medical conditions; passport and visa information for film actors and crew; internal emails; and unreleased films.

http://www.computerweekly.com/news/2240237500/North-Korea-slams-hostile-US-sanctions-over-Sony-cyber-attack?asrc=EM_EDA_38336197&utm_medium=EM&utm_source=EDA&utm_campaign=20150105_North%20Korea%20slams%20'hostile'%20US%20sanctions%20over%20Sony%20cyber%20attack_

SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Film Grid USA, 20. Nov. 15

NSA Director Adm. Michael Rogers

Paradigma Wechsel

Wir sind im Cyber-Space sehr verletzlich und werden es bleiben. Angriffe sind mit Hilfsmitteln unter 1000 $ mit entsprechendem Know-How qualifiziert möglich.

Vom reinen Schutz hin zu **Resilience**:

Resilience = Protect + Detect + Response

In der Wirtschaft ist eine Verschiebung des Investitionsvolumen zu beobachten.

Ganzheitliche Konzepte zur Cyber-Verteidigung sind gesucht.

Nur mit **Cyber-Abschreckung** ist man glaubwürdig-

SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

2. Update
ICT & Cyber-Bedrohungslage 2015
mit Schlussfolgerungen

Angela Merkel Web is Down: 7.1.2015, 14:54

Anonymous: bundestag.de, bundeskanzlerin.de down

07.01.2015

www.bundeskanzlerin.de und www.bundestag.de down. Seit einer Stunde sind die Seiten offlline, nicht mal anpingbar. Es kommt die Fehlermeldung "Server nicht gefunden". Die Hintergründe sind unklar. Eine offizielle Begründung gibt es nicht. Hat die Regierung etwa ihre Domaingebühren nicht bezahlt oder wurde die Seite gehackt?

Fakt ist, dass die Seite nicht erreichbar ist - aus welchen Gründen auch immer. So richtig vermisst wird die Seite jedoch kaum. Denn was die Blockparteien dort zu sagen haben, ist sowieso meist das Gleiche und ändern wird sich auch nichts...

Update: Anonymous steckt wohl dahinter:

Merkel Tango Down: Wir haben diese verkommene Bundesregierung gewarnt. Diese verkommene Bundesregierung wollte nicht hören. Cyberberkut und Anonymous haben www.bundeskanzlerin.de und www.bundestag.de vom Netz genommen. Wir sind Anonymous. Wir sind viele. Wir vergeben nicht. Wir vergessen nicht. Erwartet uns. #FreeUkraine

Charlie Hebdo Attack: 7. Jan. 2015

Terrorexperte Guido Steinberg im Bund:

«Man musste mit diesem Anschlag rechnen»

Der gestrige Angriff bedeutet nicht, dass die Geheimdienste nicht gut gearbeitet haben.

Könnte cyber-defence solche Attacken verhindern?

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Digitale Waffen

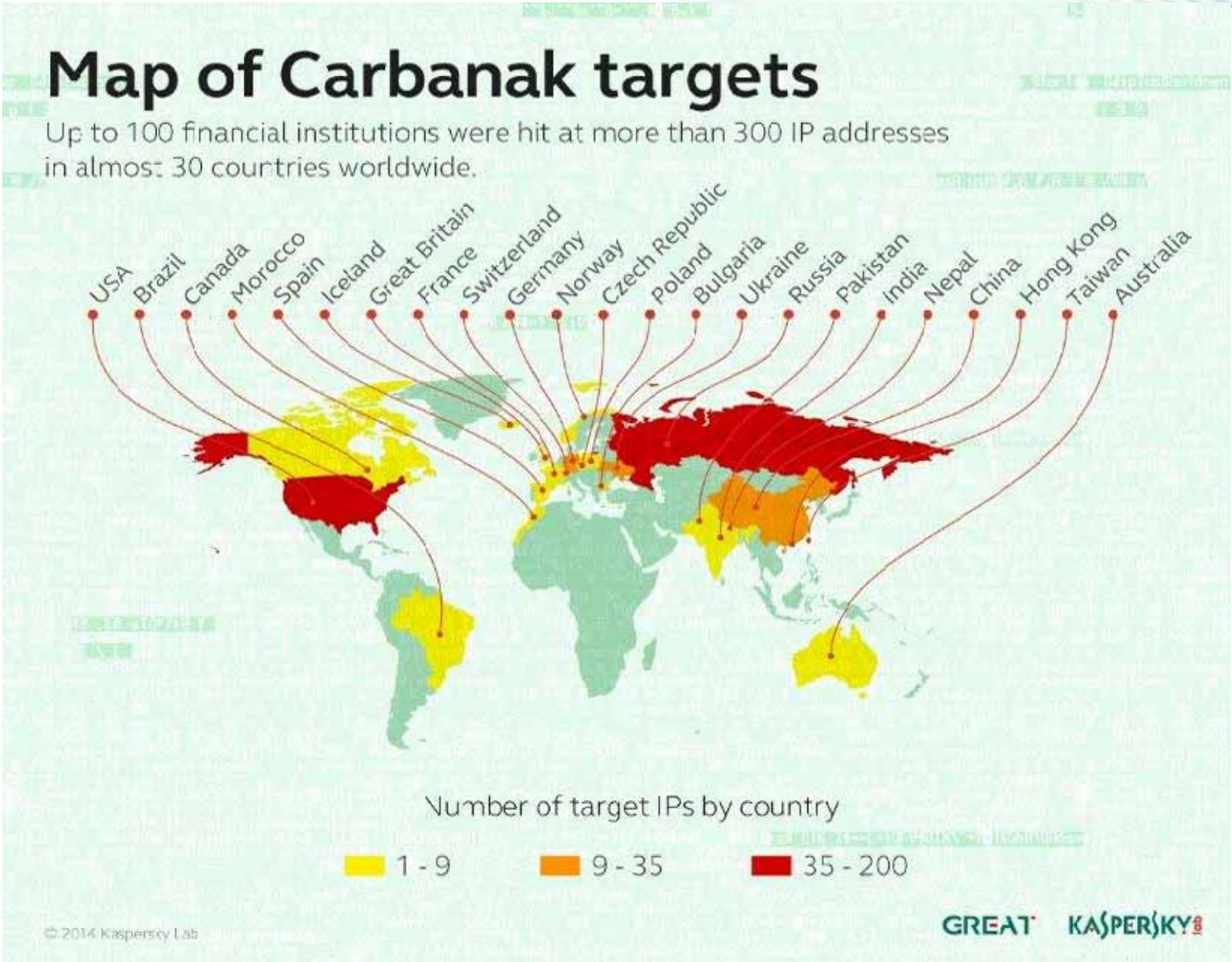
NSA baut offenbar digitale Waffen: Gemäss Edward Snowden rüstet sich die NSA für einen Cyberkrieg. Ziel sei, die eigenen Aktionen plausibel leugnen zu können.

» Von Fabian Vogt , 19.01.2015 12:12h heise.de

- Passives Datensammeln war gestern. Heute will die National Security Agency (NSA) der USA die digitale Vorherrschaft im Netz erreichen. Quelle für die Information ist das Magazin «Spiegel», dem angeblich exklusive Dokumente von Whistleblower Edward Snowden vorliegen. In den Dokumenten heisst es, dass die USA nach ABC-Waffen (Atom, biologische und chemische) nun auch **D-Waffen - digitale Waffen** - herstellen will.
- Aus diesem Grund werden offenbar für das Projekt «Politerain» «Praktikanten gesucht, die Dinge kaputt machen wollen». Zu den Jobanforderung gehört, Netzwerkkarten zu schrotten, Trojaner einzubauen oder zentrale Daten zu löschen. Das Ziel von «Politerain»: Programme wie Stuxnet aufzuziehen und dabei stets dafür zu sorgen, dass ein Unbeteiligter verdächtigt wird. Gemäss «Spiegel» soll die NSA bereits in der Lage sein, bestehende Bot-Netzte durch eigene Angriffe «umzudrehen».

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Carbanak: 1 Milliarde $ Schaden



15.02.2015 – 17:27 Uhr

Das Werk von 2 Jahren:

Der Online-Bankraub sei gemeinsam mit Interpol, Europol und Behörden verschiedener Länder aufgedeckt worden. Bis zu hundert Banken, Bezahldienste und andere Institute in rund 30 Ländern seien angegriffen worden – auch in Deutschland.

Neueste Attacken

- **26. März 2015: UPDATE: Cyber Attacker Takes Down Maine.Gov for Fourth Day Straight**
- **9. April: Hackers claiming allegiance to the Islamic State group seized control of a global French television network, simultaneously blacking out 11 channels and taking over the network's website and social media accounts …**
- Its Facebook page says its signal reaches more than 257 million homes in over 200 countries and territories. http://www.pontiacdailyleader.com/article/ZZ/20150409/NATIONWORLD/150409854

11. April 2015 shz.de **Prof. Dr. Herbert Zickfeld im Interview: „Angriffe werden dramatisch zunehmen“**
Eine aktuelle Studie der Sicherheitsberatung Corporate Trust schätzt den Schaden der Industriespionage für die deutsche Wirtschaft pro Jahr auf 11,8 Milliarden Euro. … **die Cyber-Attacke in Frankreich erst der Anfang war und die Gefahr von Wirtschafts- und Industriespionage größer wird.**

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Neuste Attacken II

Heise.de 16.4.2015

Bitkom: 51 Milliarden Euro Schaden jährlich durch digitale Wirtschaftsspionage

51 Prozent der deutschen Unternehmen waren bereits von Datendiebstahl, Sabotage oder Spionage betroffen. Besonders interessant für Angreifer ist der Automobilbau. Dies hat eine Umfrage des IT-Branchenverbands Bitkom ergeben.

EU-Kommission droht Google mit Strafe 15.4.2015

Im Streit um die Marktmacht von Google droht die EU-Kommission dem Suchmaschinenbetreiber mit einer Milliardenstrafe.

Die EU-Behörde wirft Google nun offiziell die Benachteiligung der Konkurrenz vor und verschickte am Mittwoch die Beschwerdepunkte an den US-Konzern. Damit verschärfte sie das seit 2010 laufende Verfahren. In letzter Konsequenz drohen Google ein EU-Bussgeld von aktuell bis zu **6,6 Milliarden Euro sowie Auflagen für sein Geschäftsmodell in Europa**

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Neue Lage

Atomare Waffen
Biologische Waffen
Chemische Waffen

Digitale Waffen

Elektronische Kognitivität Waffen

Schlussfolgerungen

Bedrohungslage

Die Bedrohungen sind angestiegen wegen:

- Einfacherer und billiger Produktion der Schadcodes (Eintritt 1000 US $)
- Entdeckung der kostengünstigen Wirkungserzeugung (politisch, Splittergruppen)
- Wegen dem ausdrücklichen Willen von 50+ Nationen den Cyberspace als neue Kampfdomäne zu definieren

Verteidigungslage

Wir in CH brauchen einen massiven Schub, um unsere **bewaffnete Neutralität**, **unsere Souveränität** und **unsere Prosperität** verteidigen zu können

Abhängigkeit

Fast 100% Software Abhängigkeit der Informatikanwendernation Schweiz, fast 100% Abhängigkeit der Schweiz von Hardware und Chip Lieferanten

Zum Vergleich:

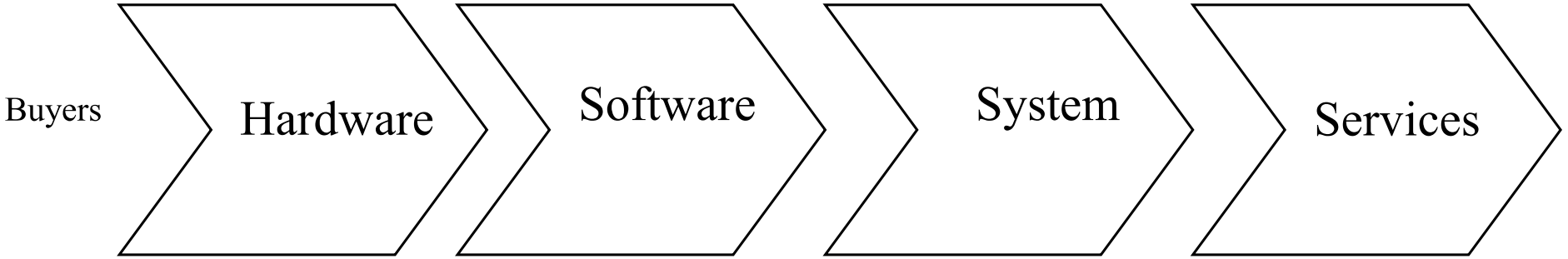
US Cyberverteidung hat ein Budget von 6 Milliarden US $

Norwegen hat 1000 Cyber-Soldaten

Die Schweiz und die Wertschöpfungskette

- **Kann die Schweiz die heutige Prosperität erhalten**
- **Zum Vergleich**
  - Kodak hat in 16 Jahren 28 Milliarden USS vernichtet und Chap. 11 angemeldet
  - Der Wechsel der SMI Firmen ist jährlich

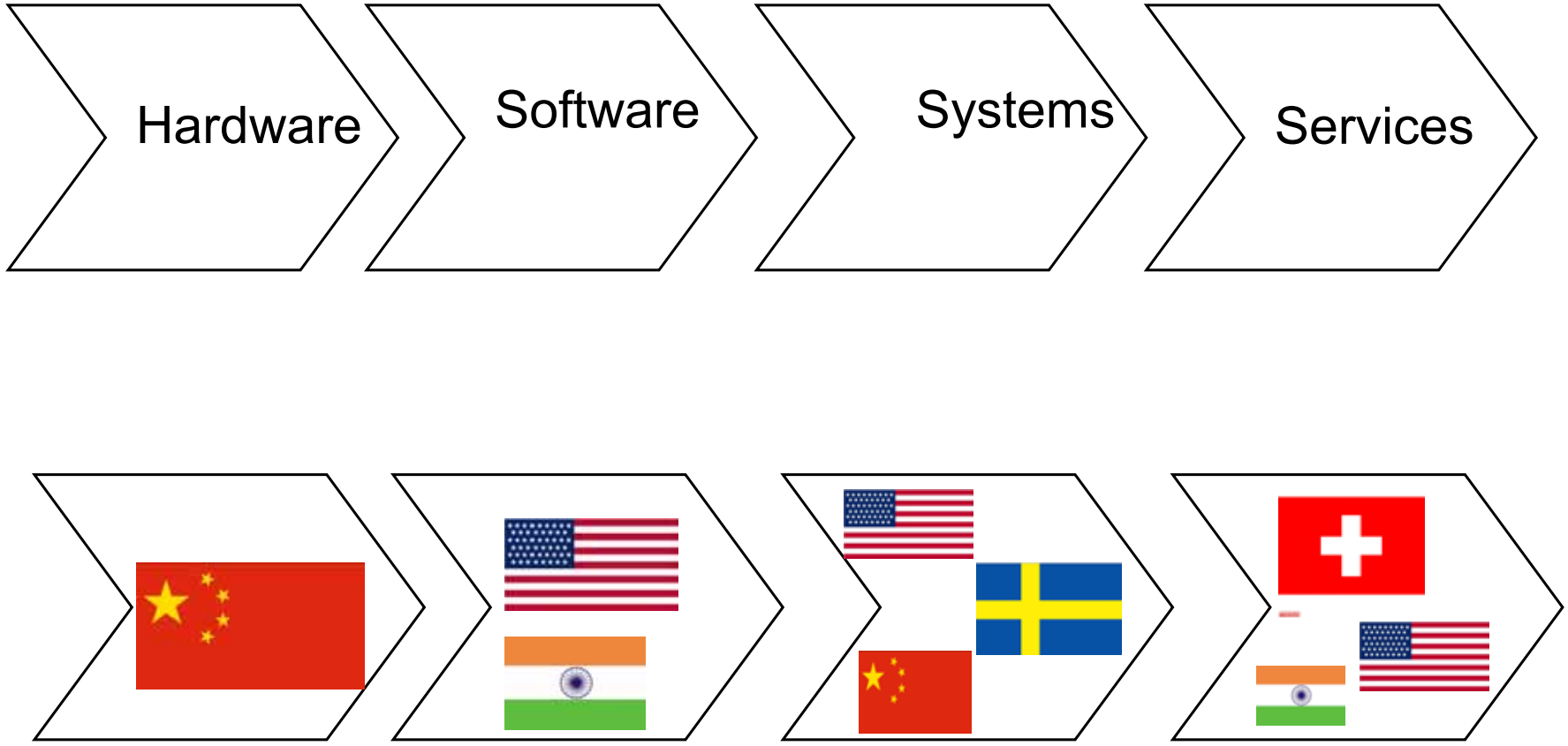
Security Value Chain
Concrete View



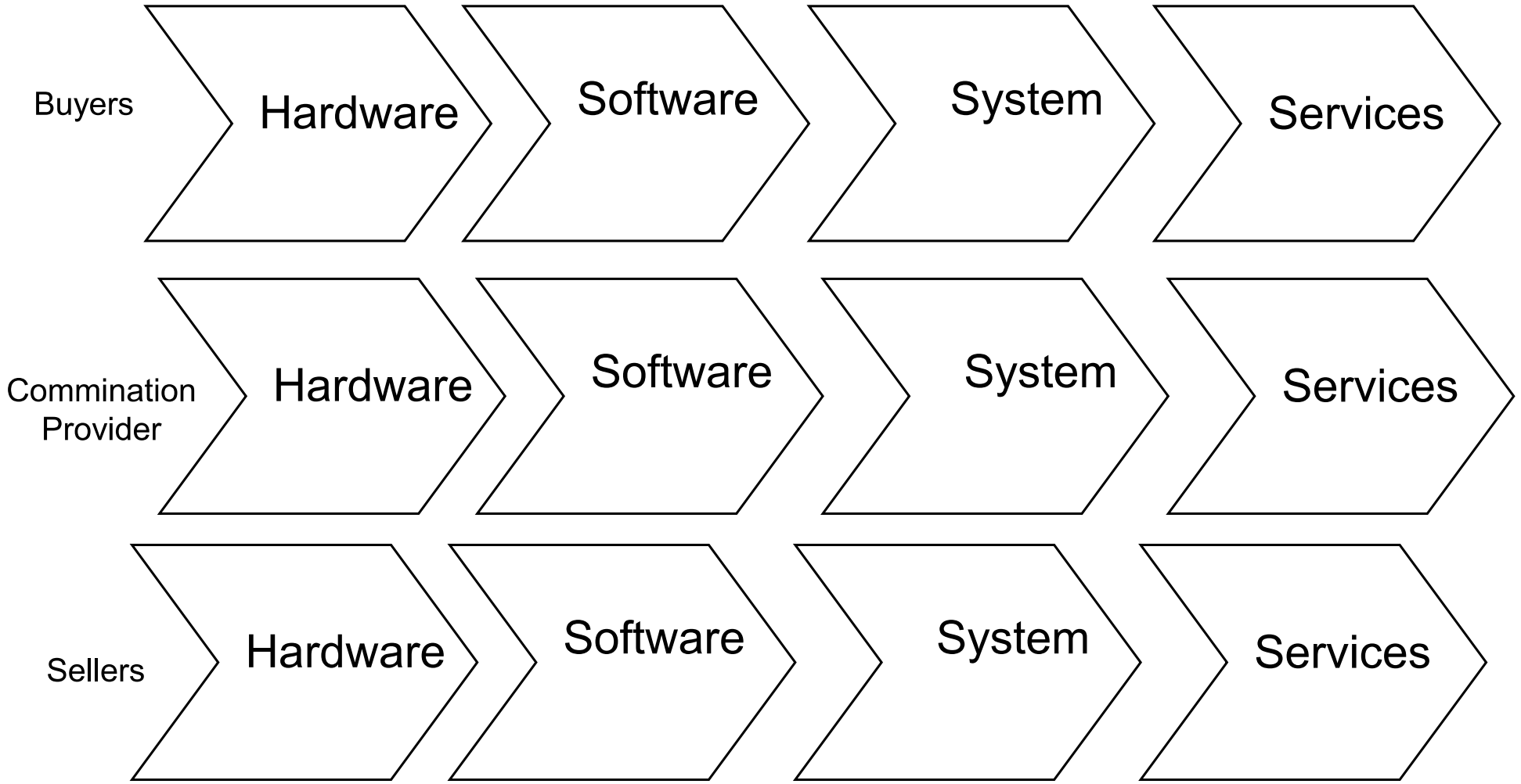
Total global market size for e-business security products in $ millions (2000–2005)

	2000	2001	2002	2003	2004	2005
Access security	940	2,160	4,830	7,850	12,690	16,120
Communication security	810	1,610	2,970	4,680	7,340	9,040
Content security	660	1,300	2,390	3,700	5,660	6,910
Security Management	700	1,520	2,790	4,460	9,490	11,820
Services	410	1,020	2,390	4,610	9,050	14,780
Total	3,520	7,610	15,370	25,300	44,230	58,670

Security Value Chain
Concrete View

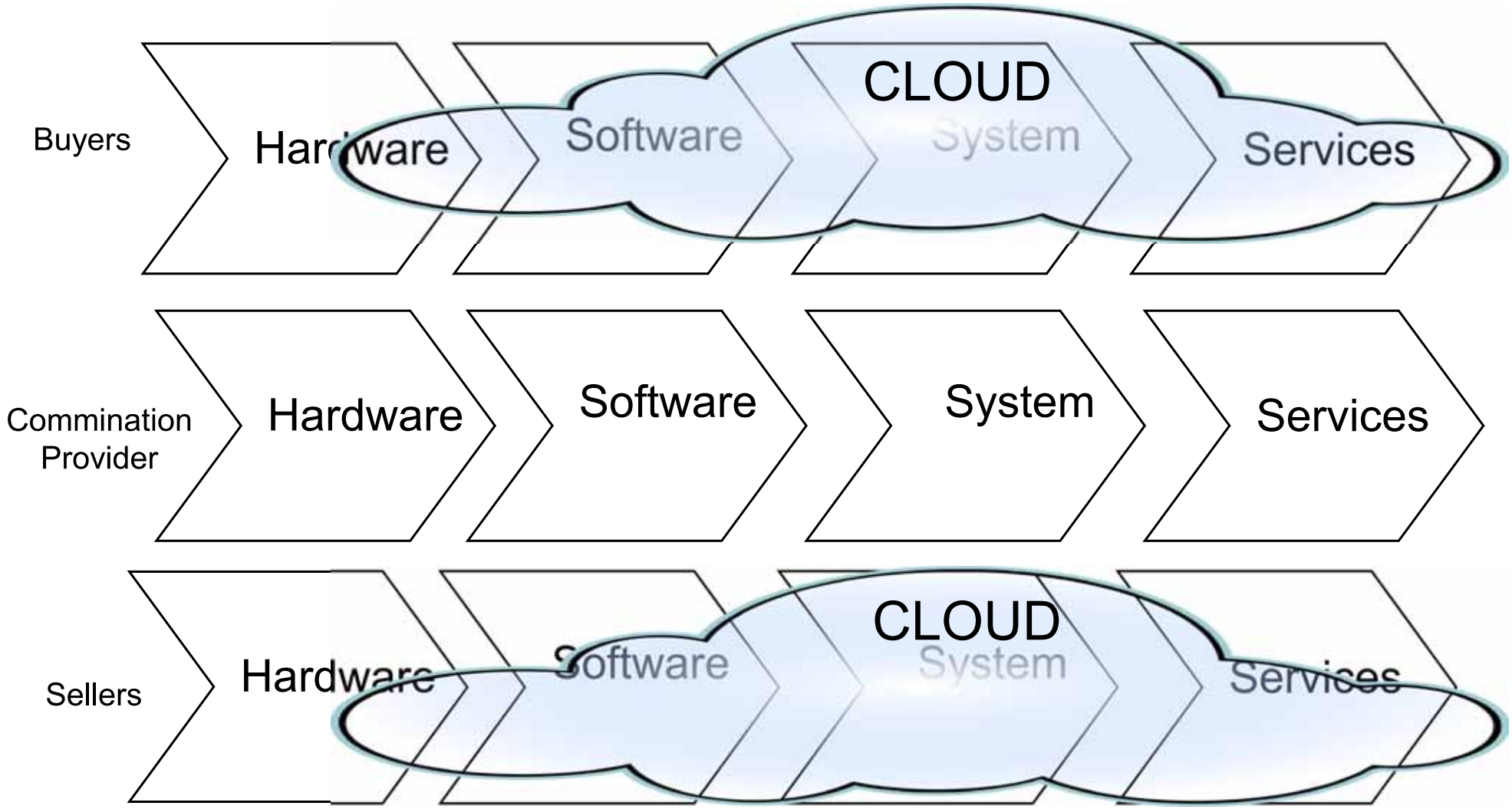


Security Value Chain
Concrete Complex View



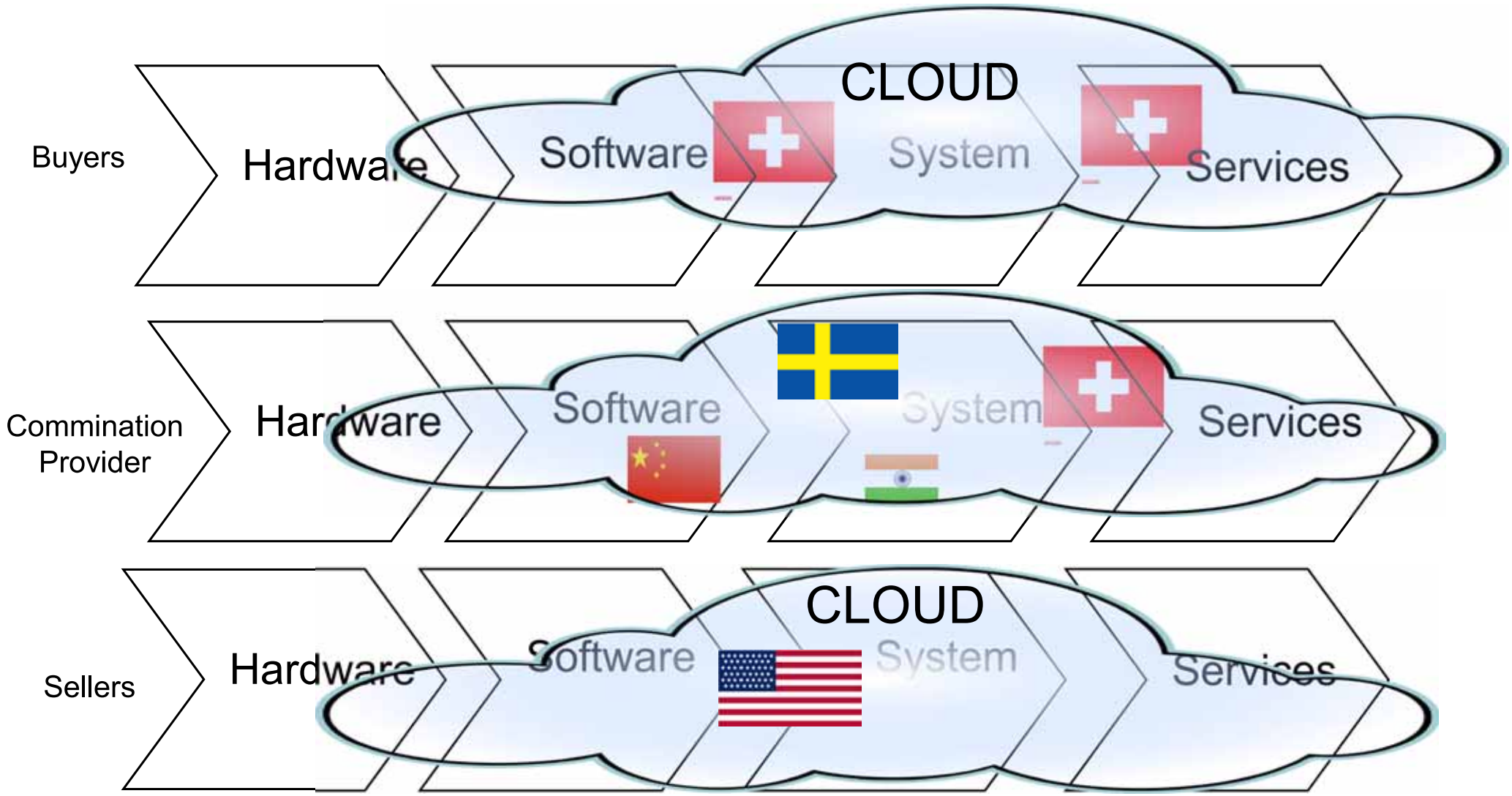
SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Security Value Chain
Concrete Complex Cloud View



SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Security Value Chain
Global Concrete Complex Cloud View



Schlussfolgerungen

- **Die Value-Creation-Chain stellt komplett neuen Anforderungen**
  - **Kodak**
  - **Buchhandel ist in der Cloud**
  - **Telefonie (Skype)**
  - **Banken ➔ FB, Google, Paypal, Amazon, Telco?**
  - **Pharma-Branche: elektronische Doktor:**
  - **berücksichtigt dieser Roche und Novartis?**

- **Wie positionieren wir uns als Schweiz?**

3. Handlungsbedarf Schweiz im Bereich Cyber-Security

Handlungsfelder

- Digitale Hoheit (**Souveränität**) erhalten:
  Wo sind die Schutzkräfte und mit welcher Drohkulisse kann die Schweiz zur glaubwürdigen Verteidigung auftrreten?
- Antworten für die aktuellen Bedrohungen finden: **Resilience**
  (Schutz mit Fehlererkennung und Behebungsmechanismen)
- **Exponentielles Wachstum** des Digitalen Raumes, mit der Fähigkeit sofort die ganze Welt als Kunde zu haben:
  Schweizer Strategie um die Gelegenheit zu nutzen und Grundlagen für künftige **Prosperität** legen
- **Geschäftsprozesse** bezüglich Risiken beurteilen und die Schweiz entsprechend positionieren.
- **Hyperkonnektivität** nur dort einsetzen, wo die Risiko-Nutzen Bilanz es erlaubt.

Fragen an die Politik

1. Welche Einsatzkräfte hat die Schweiz im Cyber-Space?
   Frankreich konnte kurzfristig 15 Experten senden
2. Wer kann in CH einen Nachweis des Täters bringen, sei es bei Fälschungen, Kriminalität oder Terror?
   ➔ Digitales Labor Analog zu ABC Labor Spiez?
3. Welche globale Strategie hat die, um sich in die neue Value-Creation-Chain einzuklinken

Aufbau unserer Veranstaltung

Die zentrale Frage ist:
Kann die Schweiz für Nischen sichere Hard- und Software liefern?

Eine Tradition an der ETHZ hat in den letzten 30 Jahren kontinuierlich an minimalen Systemen gearbeitet die sehr sicher und überblickbar sind.

In dieser Debatte werden Möglichkeiten und Bedürfnisse für Schweizer HW und SW gegeneinander abgewogen.

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Sichere ICT und Cloud aus der Schweiz: Fiktion oder Realität?

- Intro Bedrohungslage und Handlungsbedarf / Rolle der CH Wissenschaft Moderation
- *Prof. Bernhard Hämmerli SATW*
- **Wie weit können öffentliche Auftraggeber Swissness der Auftragnehmer, der Hardware und Software fordern?** *Thomas Maier, Nationalrat*
- **Native Systems Design: ein Weg zum vollständig sicheren Computer?** *Prof. Jürg Gutknecht*
- **Wie können unterschiedliche Angriffsmodelle in der Cloud erfasst und bewertet werden?** *Prof. Dr. Srdjan Capkun, ETHZ*
- **Was hat sich aber bei Cloud Computing Technologien bezüglich Schutz der Daten geändert, und welche Lösungen dürfen wir in Zukunft erwarten?** *Dr. Andreas Wespi, IBM Research*

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Sichere ICT und Cloud aus der Schweiz: Die Rolle der Wissenschaft für Lösungen und Innovation.

Paneldiskussion mit:

- Wie ist die Position der CH Wirtschaft bezüglich Swissness
  Roger Halbheer, Swisscom Chief Information Security Officer
- *Thomas Maier, Nationalrat*
- *Prof. Jürg Gutknecht*
- *Dr. Andreas Wespi, IBM Research*

Moderation: Prof. Bernhard Hämmerli SATW

Fragen / Diskussion

Während dem Panel