

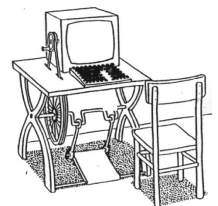
Cyber Defense Framework

(avagy megint lemaradunk valamiről?)

Biró László

CISA, CISM, CGEIT

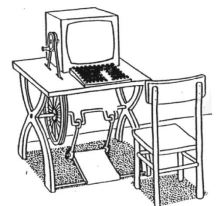
laszlo.biro@samunet.hu



NIAS – NATO Information Assurance

1997-ben – jórészt Magyarország kezdeményezésére létrejött a NATO Information Assurance Symposium, egy, az információbiztonság kérdéseivel foglalkozó egy hetes konferencia és workshop.

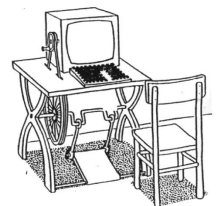
2011-ben az egyik érdekes téma a Cyber Defence Framework volt...



Miért vált szükségessé ez a keretrendszer?

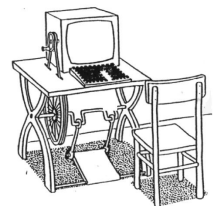
A számítógépes csintalankodás nem újkeletű és voltak – vannak fokozatai. Kezdetben az volt, hogy

- „Megmutatom, hogy be tudok jutni”
- Ha már bejutottam, hagyok is valami nyomot, amire büszke lehetek (Deface)
- Ha már egyszer ott járok, megviccelem a kollégákat...
- Haragszom a volt főnökömre, kicsit hárfázok az idegein... (DoS. stb.)



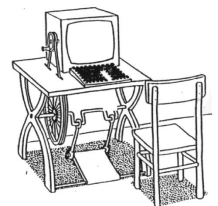
Aztán a játék komolyabbra fordult...

- Fogadjunk, hogy nem tudod kiakasztani X szolgáltatót...
- Kapsz 50 rugót, ha három napra kiakasztod Y szolgáltatót...
- Nekem megérne 100 rongyot Z közmű ügyféllistája...
- Bankkártyaszámot nem tudsz szerezni?...



Eltolódott a súlypont...

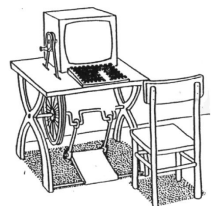
- Kósztolgassunk teljes országokat
- Szerezzünk kulcsfontosságú államigazgatási – katonai információkat
- Bénítsuk meg az államigazgatást
- Rongáljuk meg az infrastruktúrát



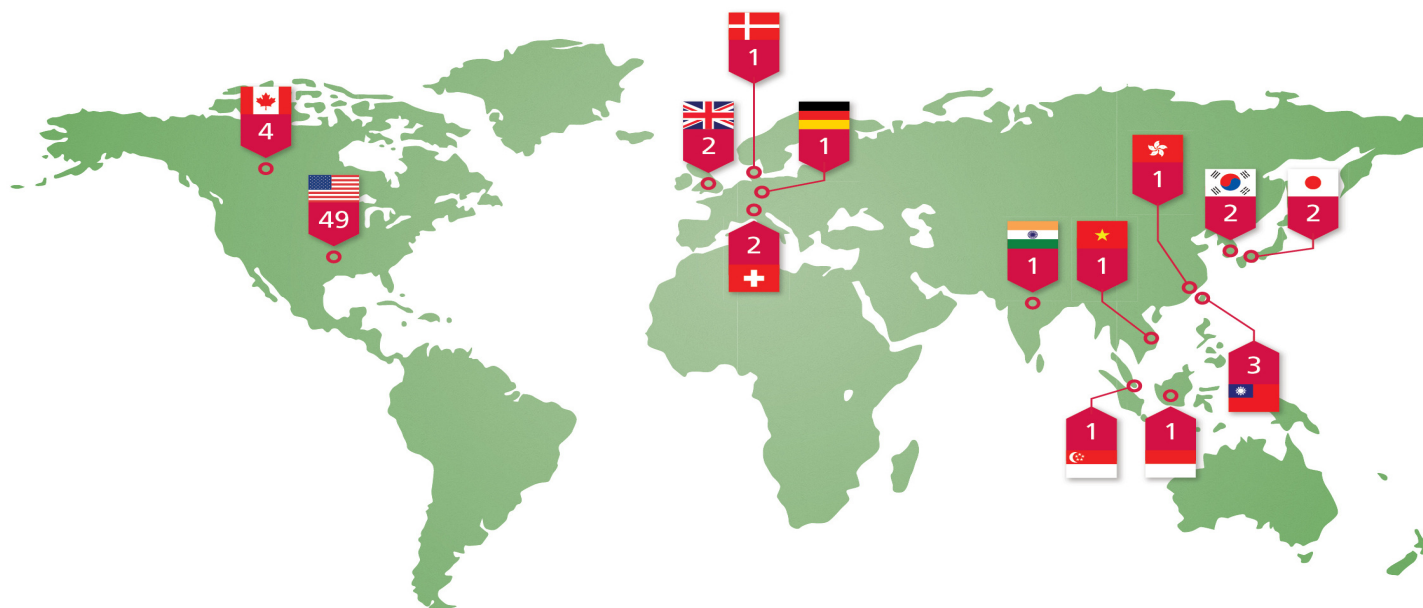
... aztán beszálltak a játékba a titkosszolgálatok is...



1982-ben „Farewell” ügynök segítségével rendeztek a Transz-Szibériai Gázvezetéken Topolszk mellett olyan tűzijátékot, ami még a világûrből is látható volt...



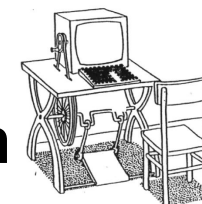
Nem csak az iparral foglalkoztak:



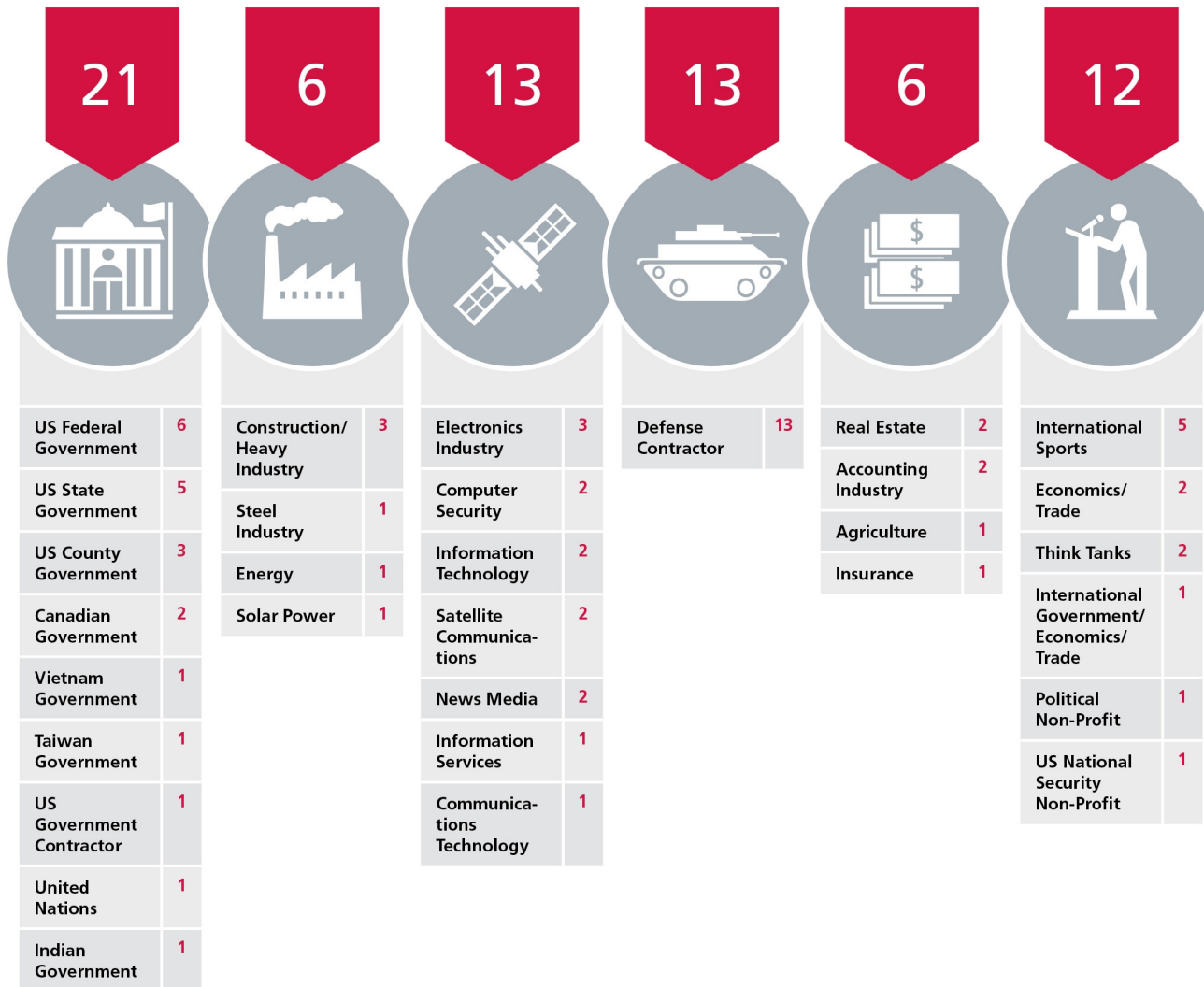
Victim's Country of Origin	Victim Count
USA	49
Canada	4
South Korea	2
Taiwan	3
Japan	2
Switzerland	2
United Kingdom	2

Source: McAfee

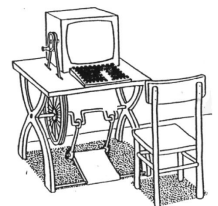
Victim's Country of Origin	Victim Count
Indonesia	1
Vietnam	1
Denmark	1
Singapore	1
Hong Kong	1
Germany	1
India	1



Mindenhova megpróbált beépülni...



Source: McAfee



...aztán egy ország teljes kommunikációs hálózata blokkolódott...

BBC NEWS

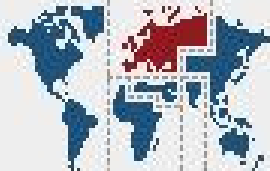
▶ Watch One-Minute World News

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

 E-mail this to a friend

 Printable version

Estonia hit by 'Moscow cyber war'



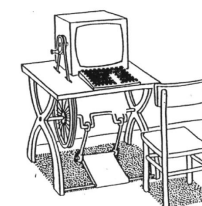
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science &
Environment
Technology

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

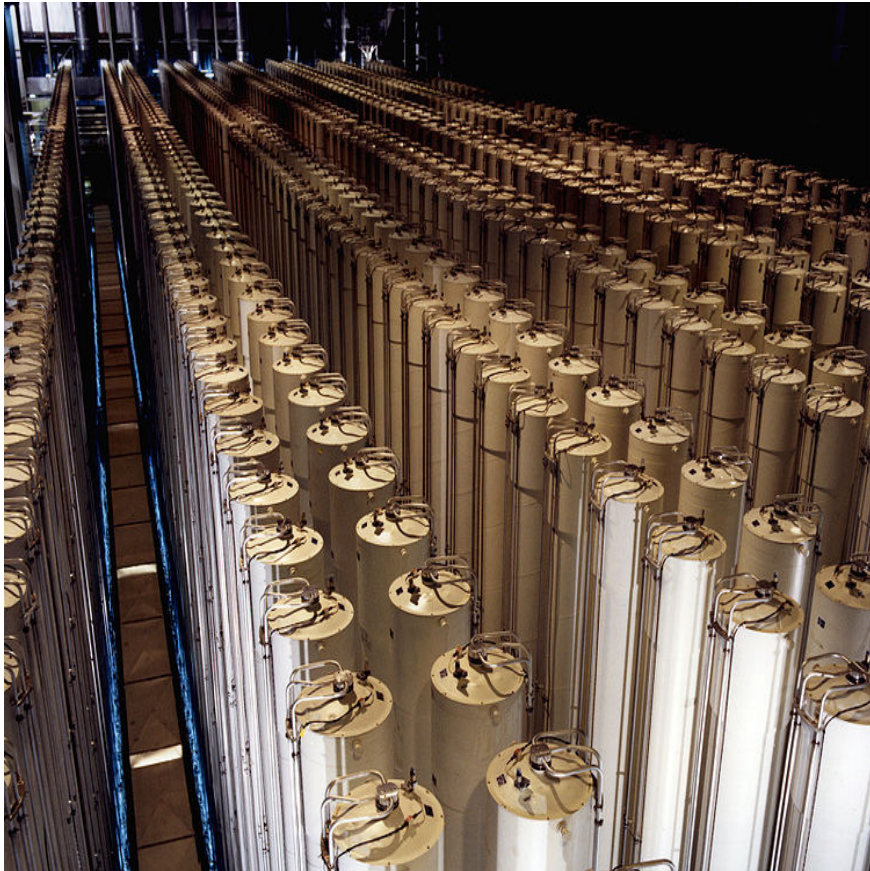
Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.



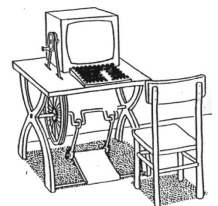
Estonia says many state websites have been affected



... és ez még csak a kezdet volt...



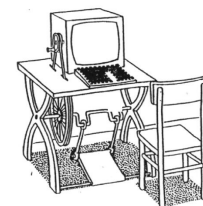
2010-ben a Stuxnet
néhány óra alatt
felszámolta Irán
urándúsító kapacitását...



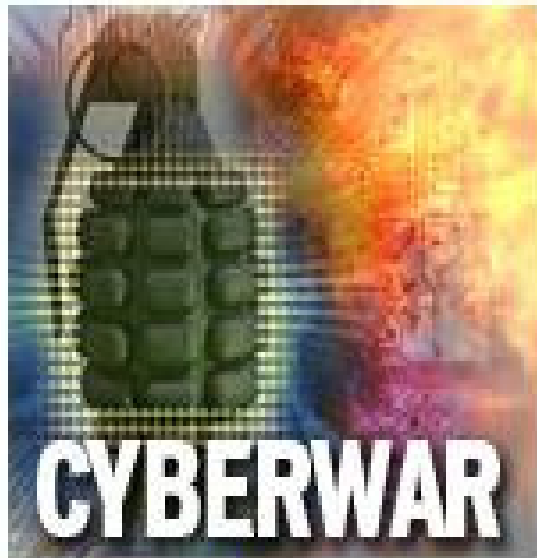
A támadási technikák megváltoztak

- A támadó kód legális, hivatalosan beszerzett programokba is beépülhetett
- A támadás bizonyos működési paraméterek együttállására, kiszámíthatatlan időben indult
- Sokszor a támadó kód szerzője sem tudta, mit alkot
- A hagyományos vírus- és behatolásvédelmi rendszerek hatástalanok voltak

Új megközelítésre, módszertanra volt szükség

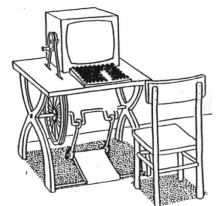


Az észtek hamar ébredtek...



After Google-China dust-up,
cyberwar emerges as a threat

Has Estonia learned much about this type of warfare in the three years since the attacks? Certainly. But in this edited interview with Aaviksoo, he says that in some ways, the country could be doing more to prepare for the next major cyberincident, which he says will inevitably come about.

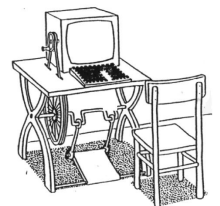


Létrehoztak Tallinban egy nemzetközi tudásközpontot



CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia





CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

+

CD Capability Framework = ???



Disclaimer

*The opinions expressed are those of the
presenter and
should not be considered as official policy of
the CCD COE or NATO*



Agenda

- Cooperative Cyber Defence Centre of Excellence
- CD Capability Framework
- CCD COE + CD CF = ???



CCD COE + CD CF = ???

CCD COE =

**= Cooperative Cyber Defence
Centre of Excellence**

- **www.ccdcoe.org**



The Cooperative Cyber Defence Centre of Excellence *Is*

- A multinationally manned and sponsored entity currently comprised of 8 Sponsoring Nations
 - *Germany, Hungary, Italy, Latvia, Lithuania, Slovak Republic, Spain and Estonia*
 - *joining process with: Turkey, USA*
- Accredited as the NATO COE (Oct 28th 2008)
- Directed and tasked by a Multinational Steering Committee of those 8 Sponsoring Nations + Turkey + NATO ACT
- Actively receives additional NATO requests via Supreme Allied Command of Transformation



Cooperative Cyber Defence Centre of Excellence *is Not*

- Part of NATO Command or Force Structure
- Funded from NATO Common budget
- 24/7 NATO Operational Incident Handling Center
nor
Multinational Computer Emergency Response Team
working on behalf of Sponsoring Nations
- Group of hackers or “Cyber Warriors”



Cooperative Cyber Defence Centre of Excellence – CCD COE

Mission and Vision



Mission: to enhance the cooperative cyber defence capability of NATO.

Vision: to become a primary source of expertise for NATO in cooperative cyber defence-related matters.



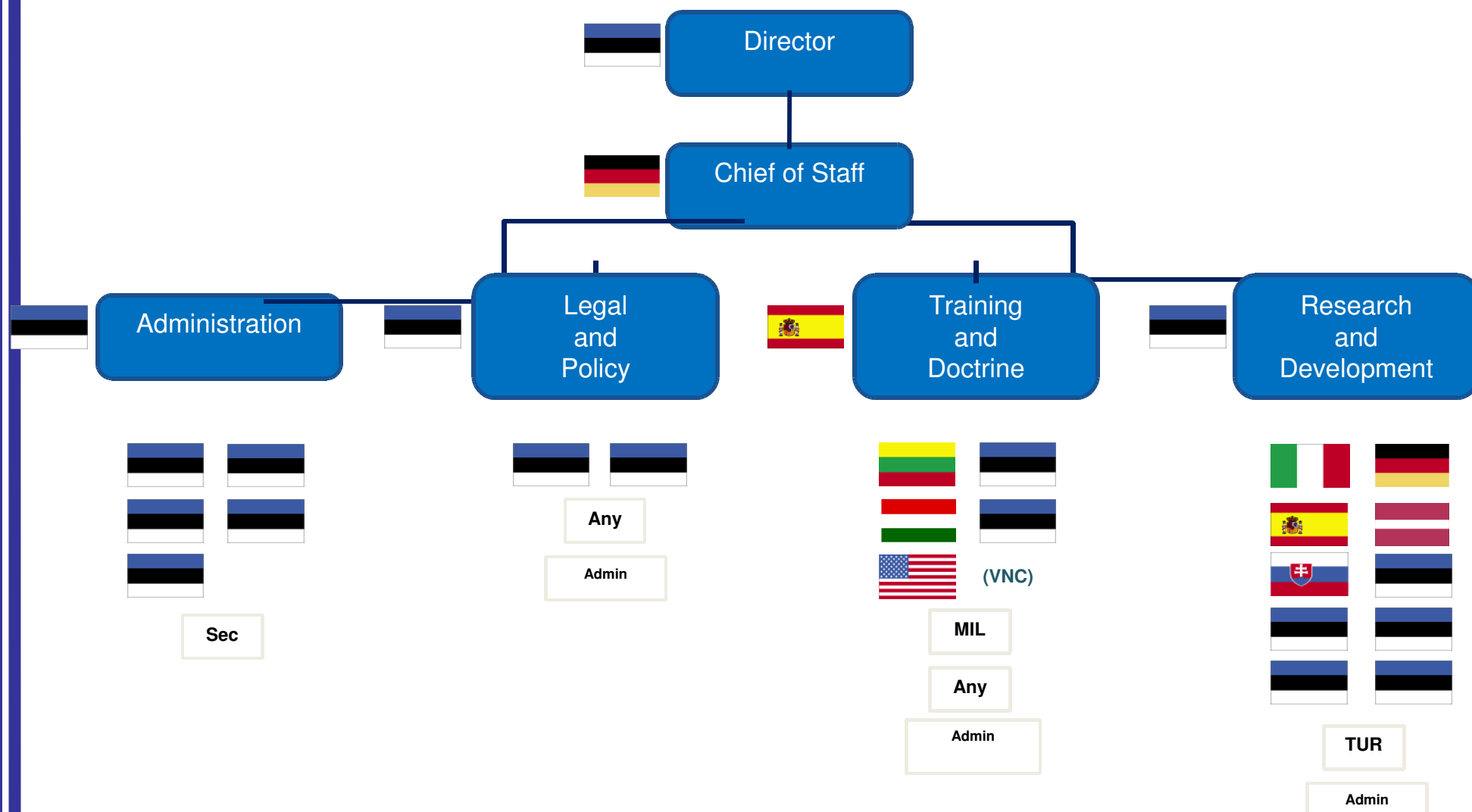
Main Functions

- **Input to doctrine and concepts in the field of cyber defence**
- **Cyber defence related analysis, education, awareness and training**
- **Research and development projects in the field of cyber defence**
- **Cyber defence related analysis and lessons learned**





Organization





Relationships



NATO entities

- HQ SACT
- NATO CDMA
- NCIRC
- NC3A

Other entities

- Universities
- Private sector

Customers

- NATO
- Sponsoring Nations
- Contributing Participants

NATO COE-s

- COE-DAT
- C2 COE

Nations

- NATO
- Non-NATO



CCD COE + CD CF = ???

CCD COE =

**= Cooperative Cyber Defence
Centre of Excellence**

- **www.ccdcoe.org**



CCD COE + CD CF = ???

??? = !!!

! = Collaboration

! = Collaboration

! = Collaboration

A NATO természetesen felkarolta a kezdeményezést



NATO Consultation, Command and Control Agency
Agence de consultation, de commandement et de contrôle de l'OTAN

Geir HALLINGSTAD

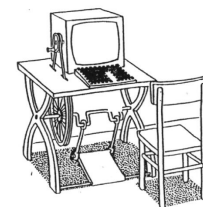
Principal Scientist

Cyber Defence and Assured Information Sharing (CAT2)

Oude Waalsdorperweg 61
2597 AK The Hague
(P. O. Box 174 2501 CD)
Netherlands
www.nc3a.nato.int

NCN 257 3742
Tel. +31 (0)70 374 3742
Fax +31 (0)70 374 3079
geir.hallingstad@nc3a.nato.int

Hallingstad úr így számolt be róla 2011-ben:





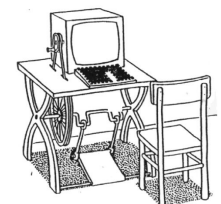
Cyber Defence Framework

Definitions and descriptions of cyber defence capabilities



• **Date: 22-09-2011**

NATO
UNCLASSIFIED



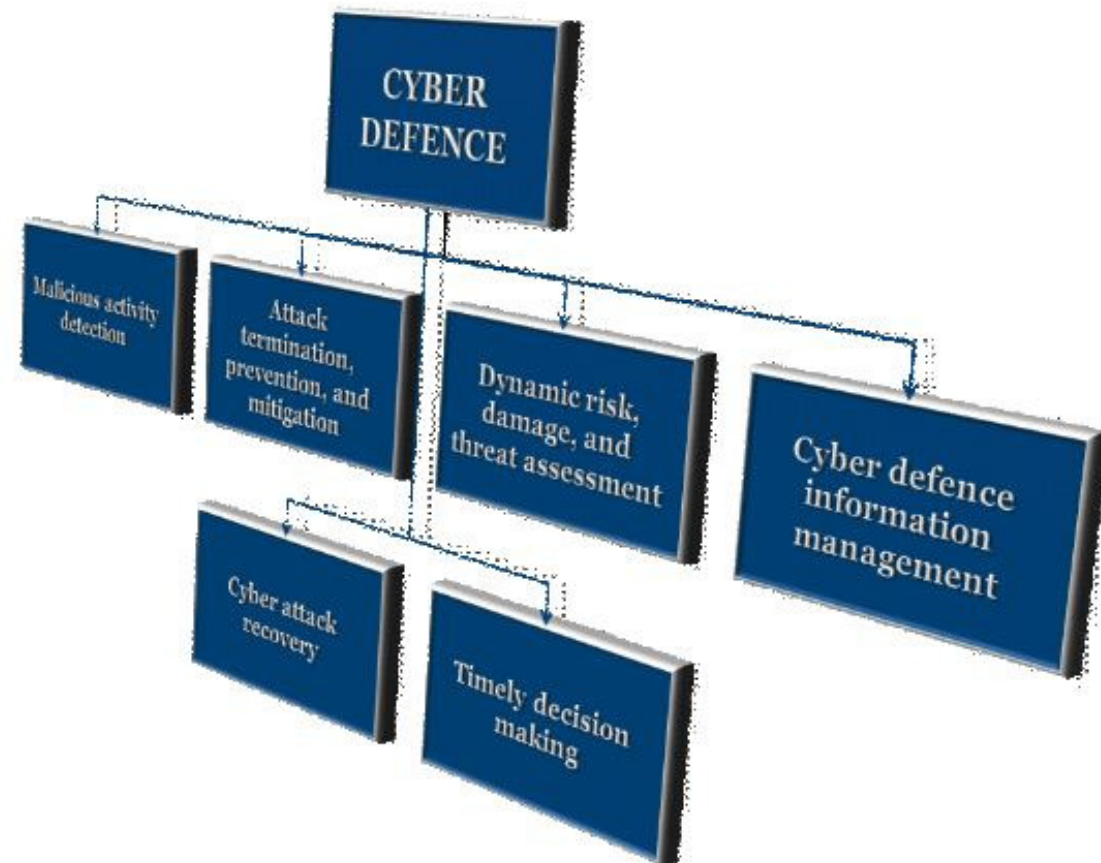
Cyber Defence Capability Framework

- **Objectives**

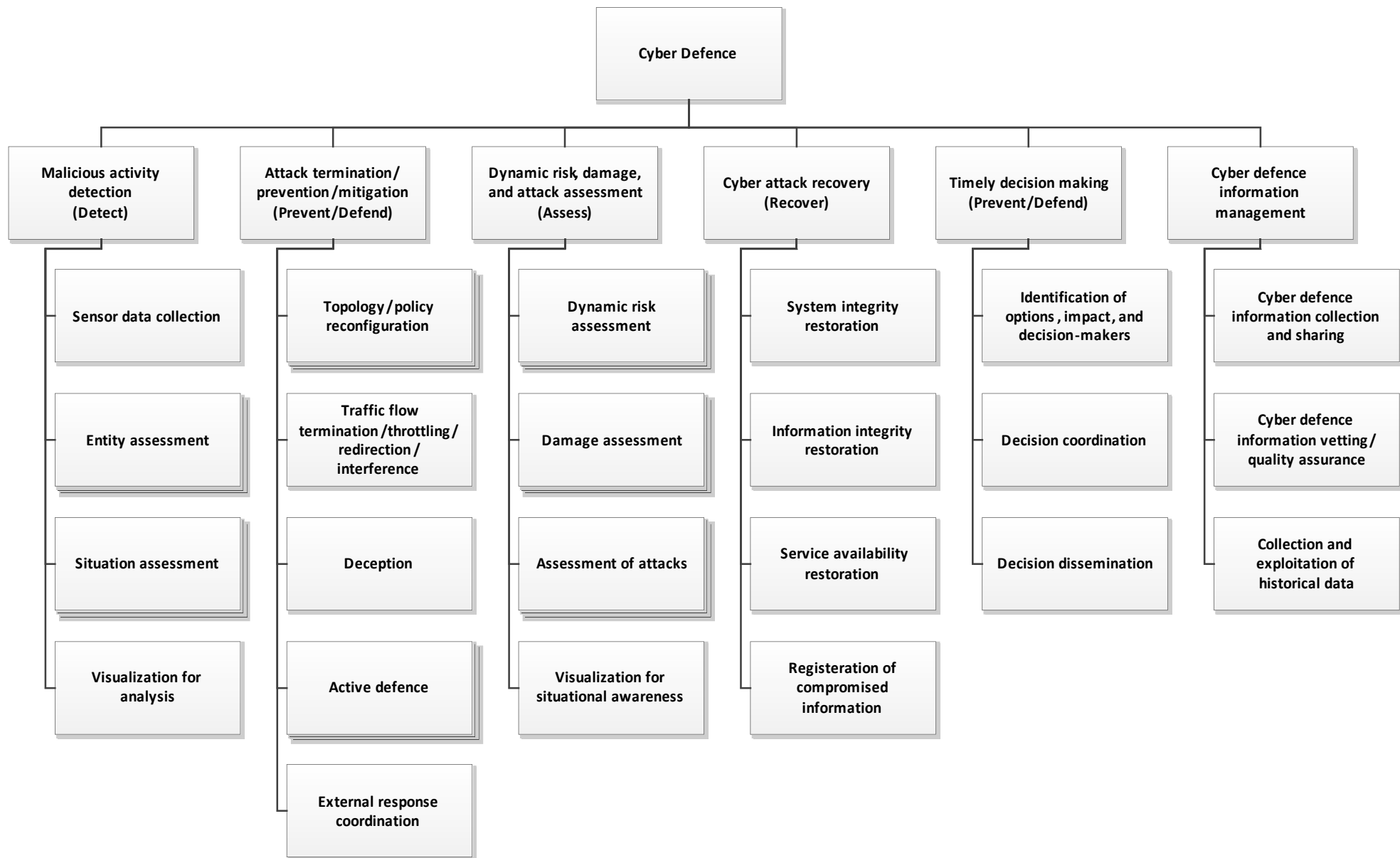
- Establish the scope of cyber defence and the capabilities that are needed for a sound overall cyber defence capability
- Provide a common taxonomy for more efficient discussion and coordination of cyber defence activities
- Provide a framework for multinational cooperation on the development of cyber defence capabilities
- Provide a framework for establishing interoperability interfaces and maturity levels for the capabilities

What is the Capability Breakdown

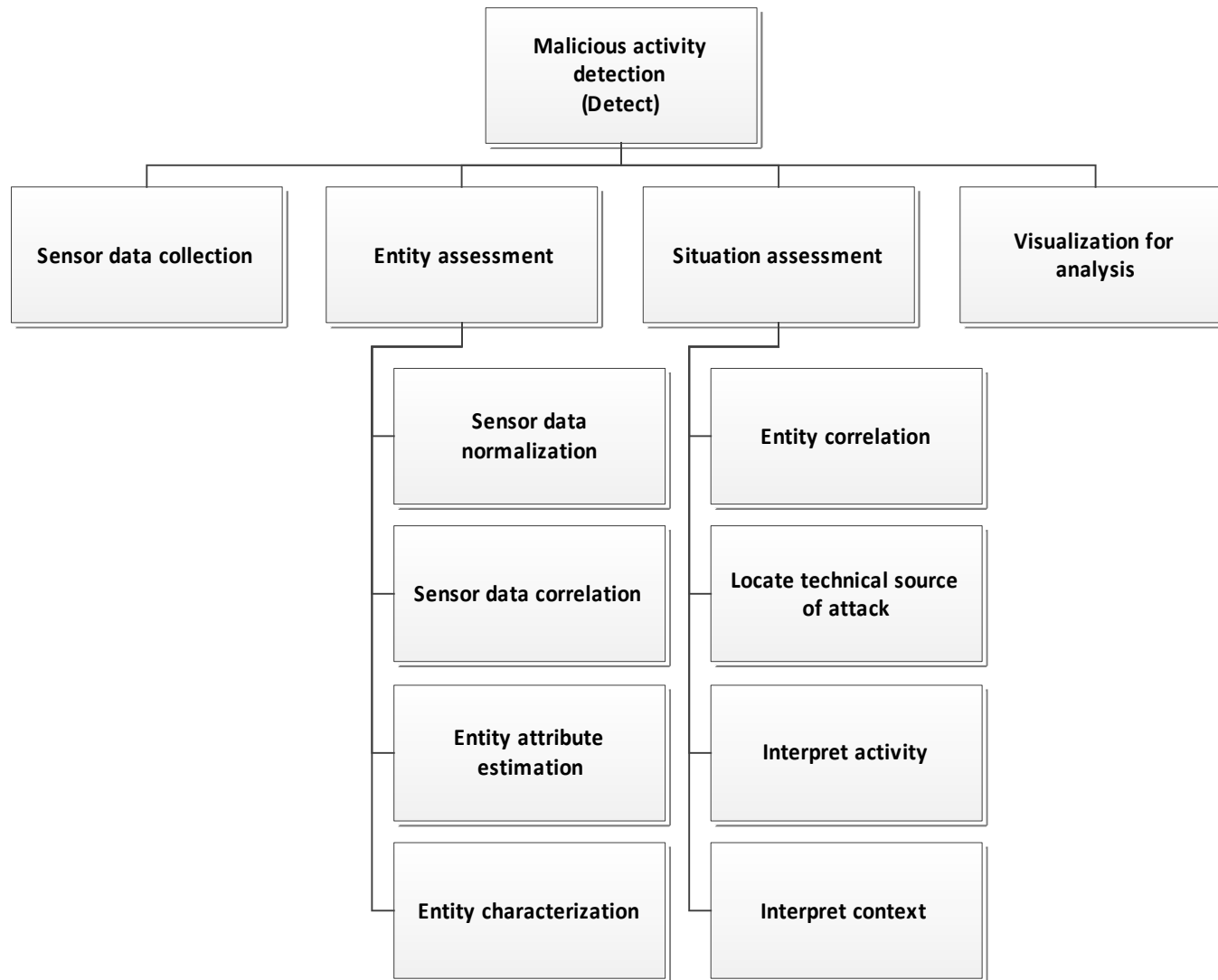
- **Capability**
 - The power/ability to do something
- **Hierarchical**
 - Structured capability breakdown
- **Does not address**
 - Processes; the order in which capabilities are used
 - Organization; who does what



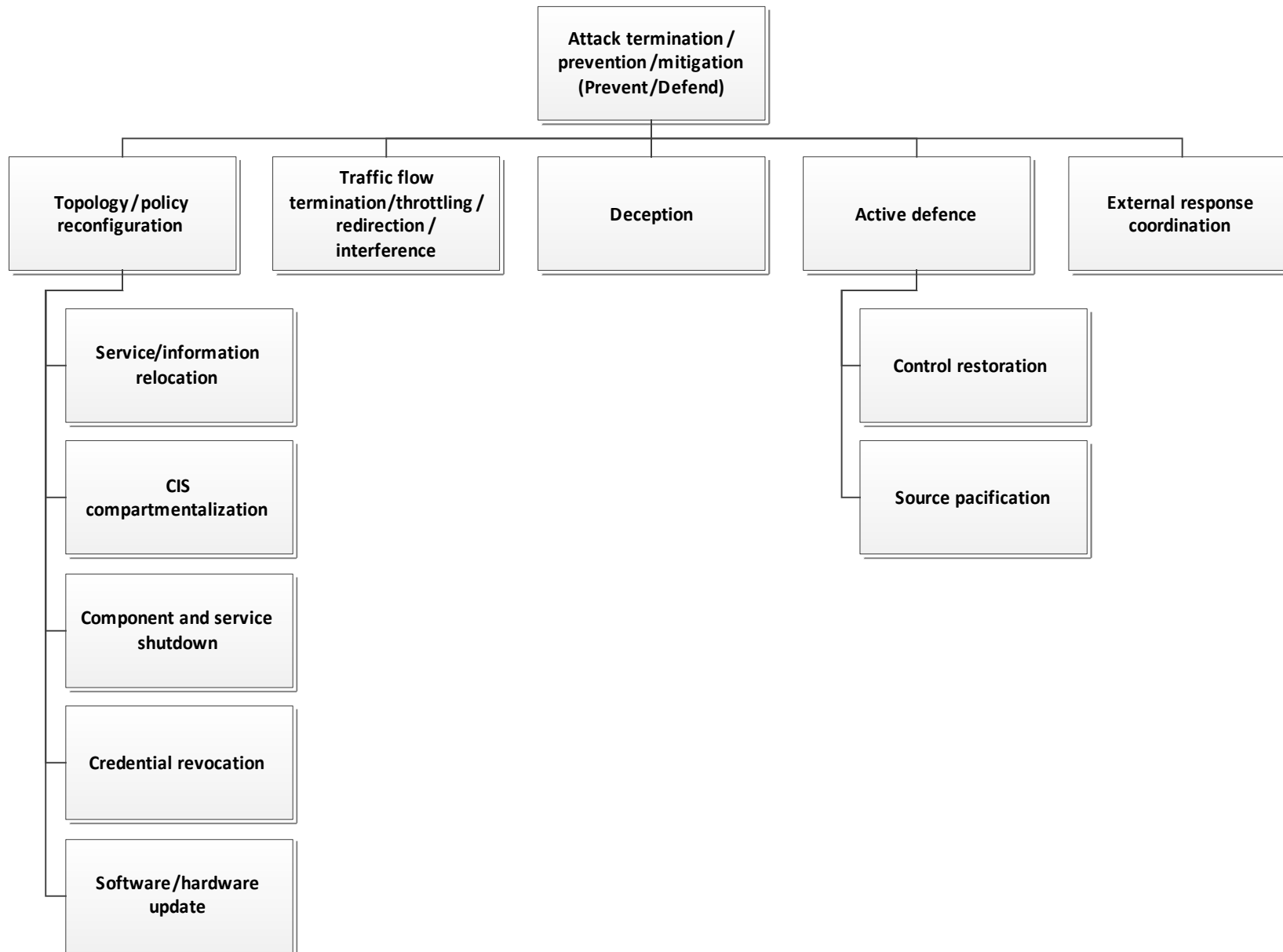
Cyber Defence Capability Breakdown



Malicious Activity Detection



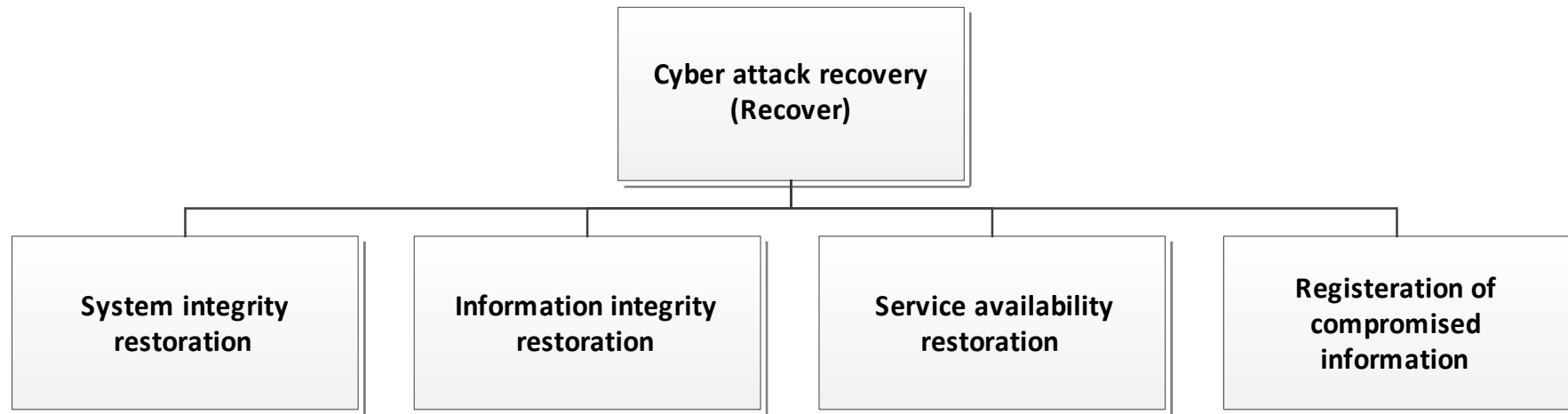
Attack termination, prevention, mitigation



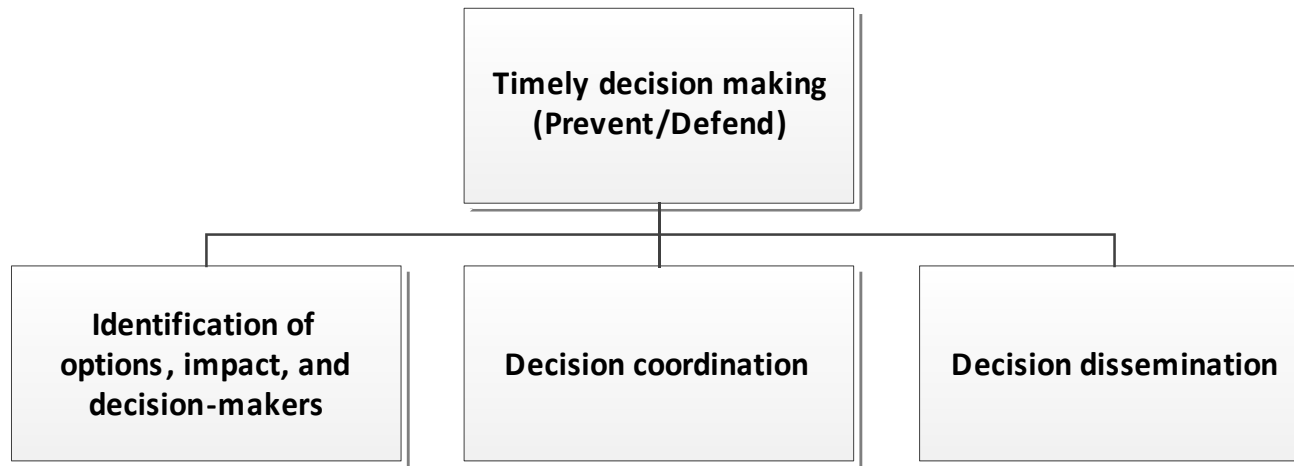
Dynamic Risk, Damage, and Threat Assessment



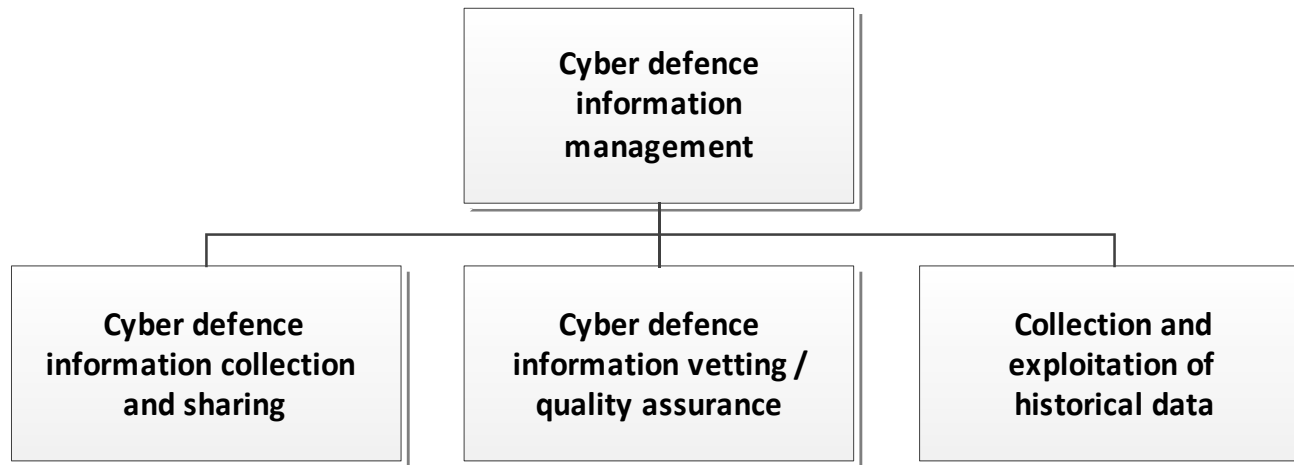
Cyber Attack Recovery



Timely Decision Making



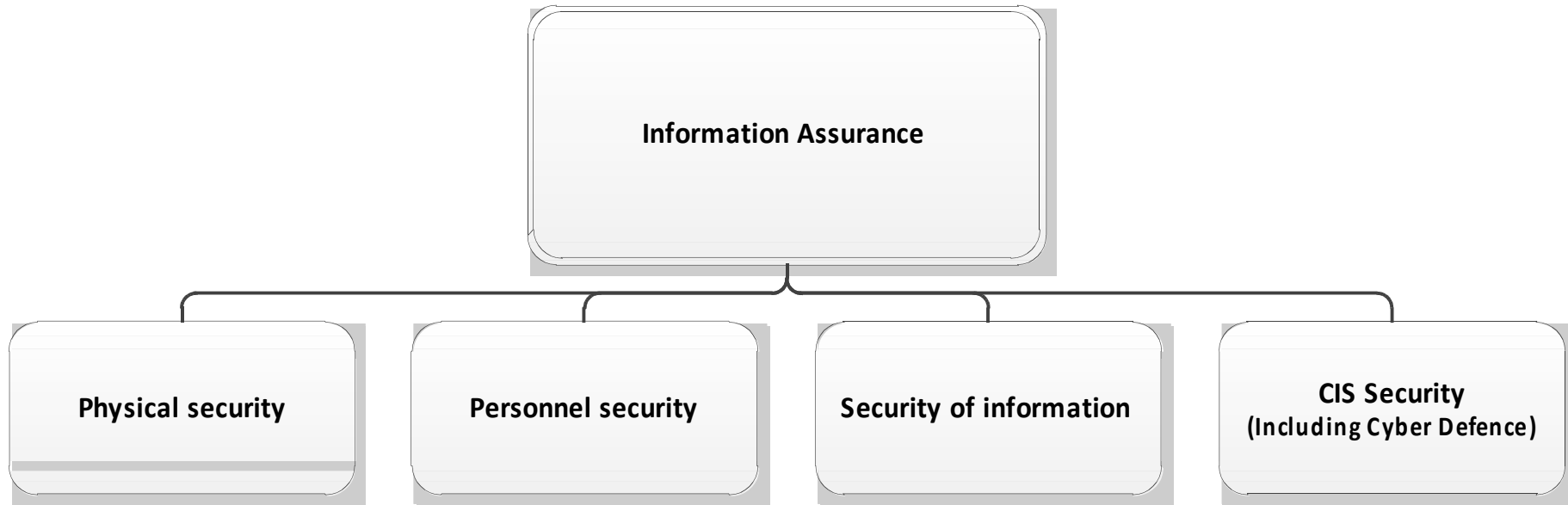
Cyber Defence Information Management



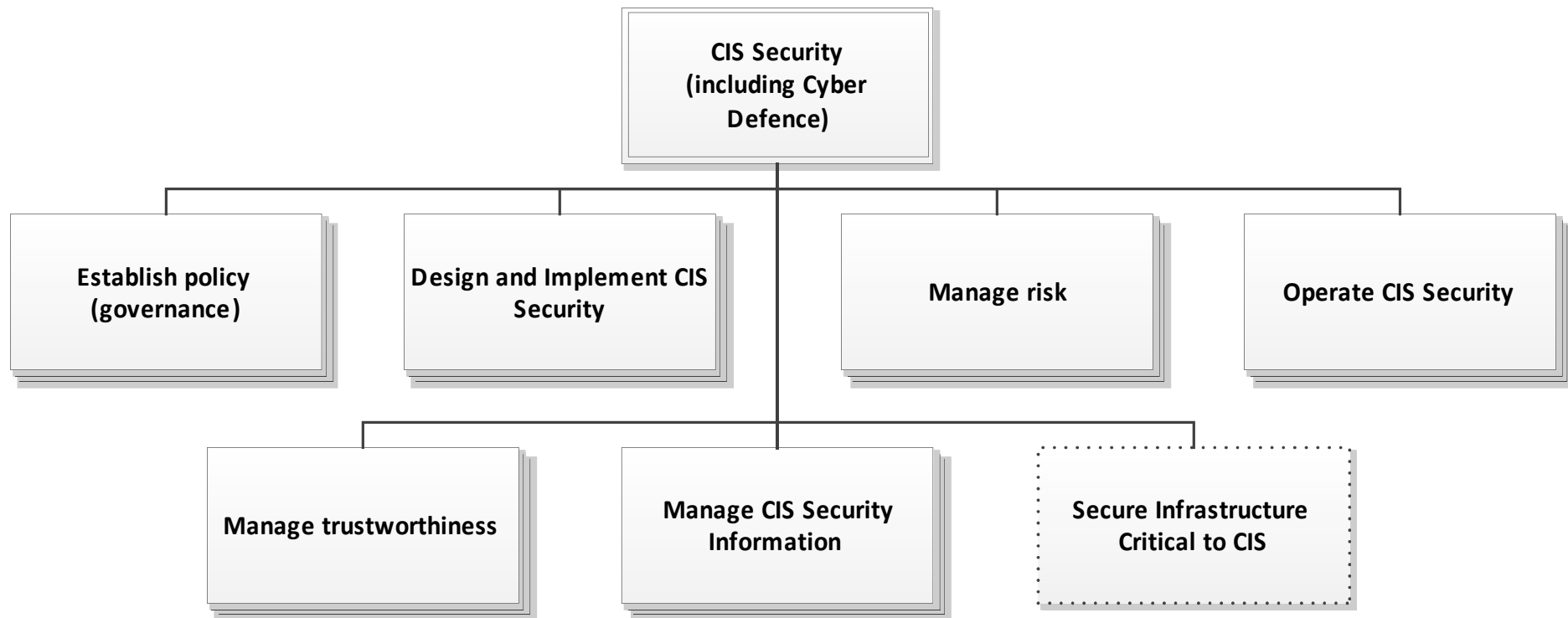
Cyber Defence User Applications

- Damage assessment
- Attack assessment
- Recognized cyber picture
- Cyber attack recovery
- Cyber course of action
- Cyber decision coordination and dissemination
- Cyber defence data exchange and collaboration
- Collection management
- Cyber analysis
- Cyber operations management
- CIS configuration management
- Cyber deception
- Dynamic risk assessment
- Malware assessment

Context for Cyber Defence

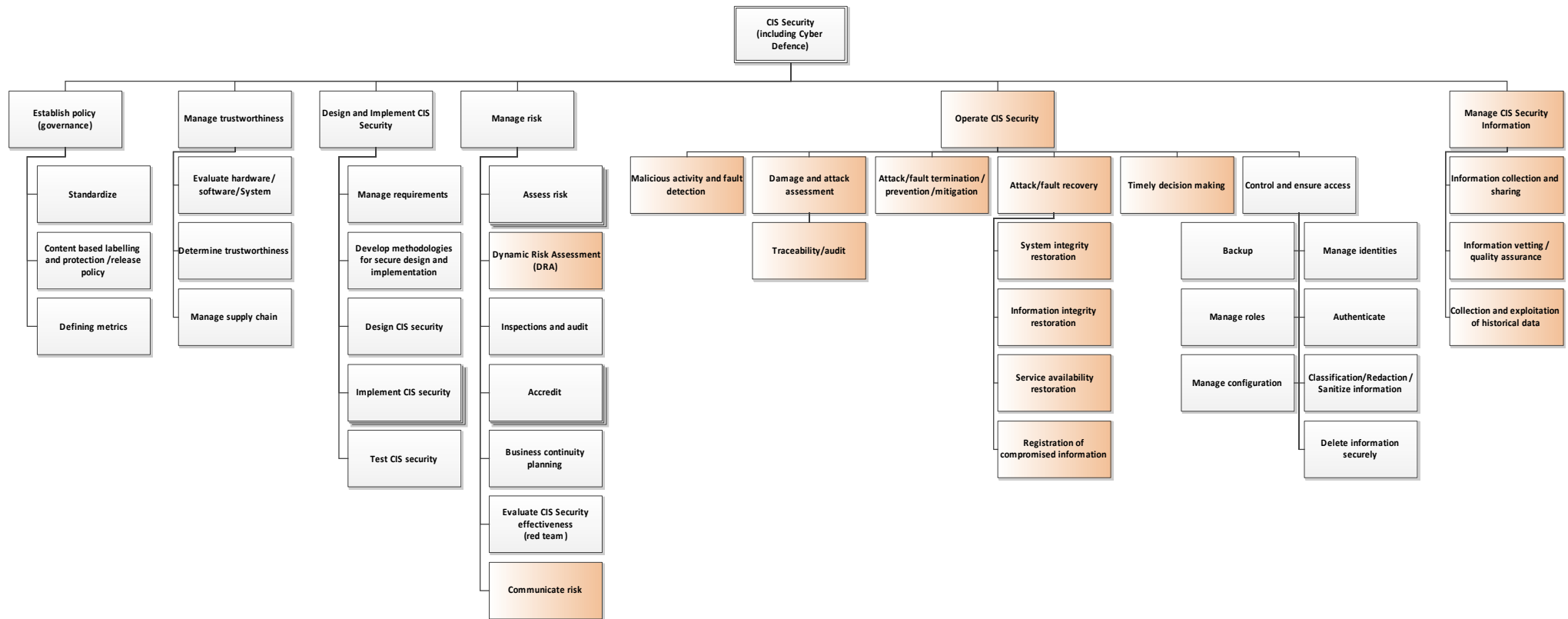


CIS Security (including Cyber Defence) Capability Breakdown



Work in progress ...

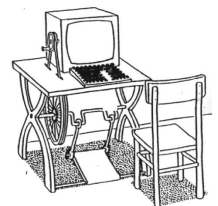
Cyber Defence as part of CIS Security



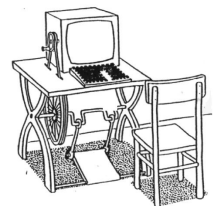
Work in progress ...

Miért jó ez nekünk?

- Egységes keretrendszer ad az események kezeléséhez
- Le tudja csökkenteni az improvizatív szakaszokat
- Rendszerezetté teszi a felkészülést az esetleges támadásokra, rendkívüli eseményekre

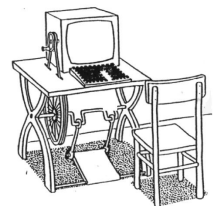


Az elkészült anyagok hozzáférhetők:



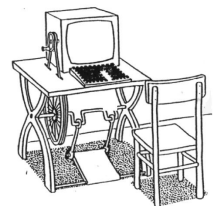
Kik használják a tudásközpont eredményeit?

AUSTRALIA	2
CYBER SECURITY STRATEGY	3
CANADA	24
CANADA'S CYBER SECURITY STRATEGY.....	25
CZECH REPUBLIC	34
CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR THE 2011 – 2015 PERIOD.....	35
GERMANY	40
NATIONAL PLAN FOR INFORMATION INFRASTRUCTURE PROTECTION.....	41
CYBER SECURITY STRATEGY FOR GERMANY	48
ESTONIA	54
CYBER SECURITY STRATEGY	55
FRANCE	76
FRENCH STRATEGY FOR THE DEFENCE AND SECURITY OF INFORMATION SYSTEMS	77
UNITED KINGDOM	84
CYBER SECURITY STRATEGY OF THE UNITED KINGDOM	85
JAPAN	100
INFORMATION SECURITY STRATEGY FOR PROTECTING THE NATION.....	101
NETHERLANDS	112
THE NATIONAL CYBER SECURITY STRATEGY (NCSS)	113
NEW ZEALAND	120
NEW ZEALAND'S CYBER SECURITY STRATEGY	121
POLAND	128
THE STRATEGY FOR THE DEVELOPMENT OF THE INFORMATION SOCIETY IN POLAND UNTIL 2013	129
USA	154
THE NATIONAL STRATEGY TO SECURE CYBERSPACE.....	155
COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS	198
INTERNATIONAL STRATEGY FOR CYBERSPACE	212
DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE	228
SOUTH AFRICA	236
CYBERSECURITY POLICY OF SOUTH AFRICA.....	237



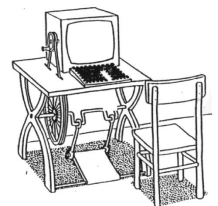
**Ki NEM használja jelenleg a
tudásközpont eredményeit?**

Magyarország!



Kérdések?...

laszlo.biro@samunet.hu





Thank you for your patience.
Köszönöm a türelmet!

