Cyber Defense Framework

(avagy megint lemaradunk valamiről?)

Biró László

CISA,CISM, CGEIT

laszlo.biro@samunet.hu

ISACA®
Serving IT Governance Professionals

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 újkeletû 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 fõnökömre, kicsit hárfázok az idegein... (DoS. stb.)

ISACA
Serving IT Governance Professionals

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 közmû ügyféllistája...

- Bankkártyaszámot nem tudsz szerezni?...

ISACA®
Serving IT Governance Professionals

Eltolódott a súlypont...

- Kóstolgassunk teljes országokat

- Szerezzünk kulcsfontosságú államigazgatási – katonai információkat

- Bénítsuk meg az államigazgatást

- Rongáljuk meg az infrastruktúrát

ISACA®
Serving IT Governance Professionals

… aztán beszálltak a játékba a titkosszolgálatok is...

1982-ben „Farewell” ügynök segítségével rendeztek a Transz-Szibériai Gázvezetéken Topolszk mellett olyan tüzijátékot, ami még a világûrbõl 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

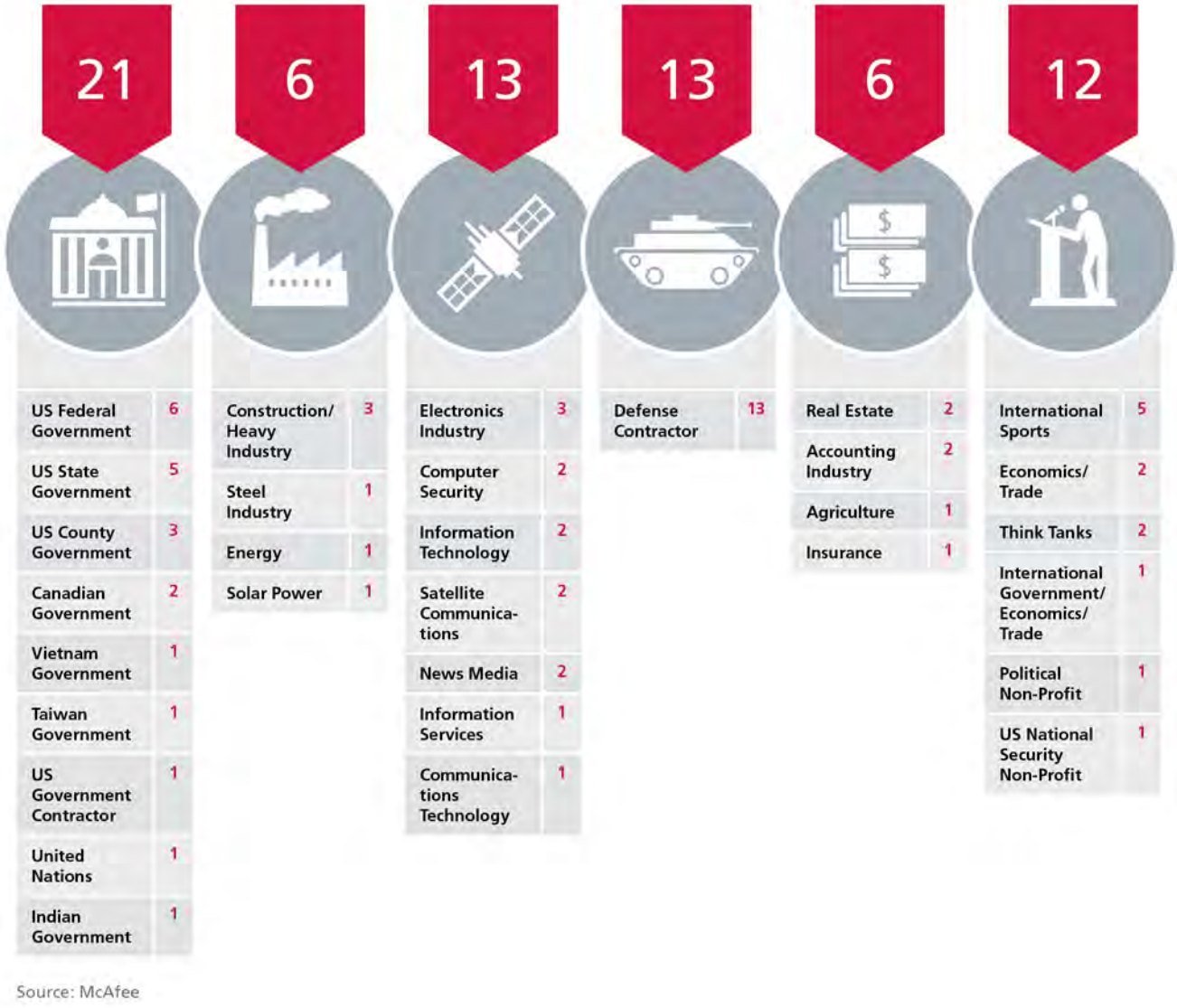
Victim's Country of Origin	Victim Count
Indonesia	1
Vietnam	1
Denmark	1
Singapore	1
Hong Kong	1
Germany	1
India	1

Source: McAfee

ISACA
Serving IT Governance Professionals

2006-ban a ShadyRat végigsöpört a fél világon

Mindenhova megpróbált beépülni...



Source: McAfee

ISACA
Serving IT Governance Professionals

Totális támadás volt

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

BBC NEWS

Watch One-Minute World News

News Front Page

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

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'

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

ISACA
Serving IT Governance Professionals

… és ez még csak a kezdet volt...

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

ISACA®
Serving IT Governance Professionals

A támadási technikák megváltoztak

- A támadó kód legális, hivatalosan beszerzett programokba is beépülhetett

- A támadás bizonyos mûködési paraméterek együttállására, kiszámíthatatlan idõben indult

- Sokszor a támadó kód szerzõje 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.

ISACA
Serving IT Governance Professionals

Létrehoztak Tallinban egy nemzetkõzi tudásközpontot

CCDCOE

Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

ISACA®
Serving IT Governance Professionals

+

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

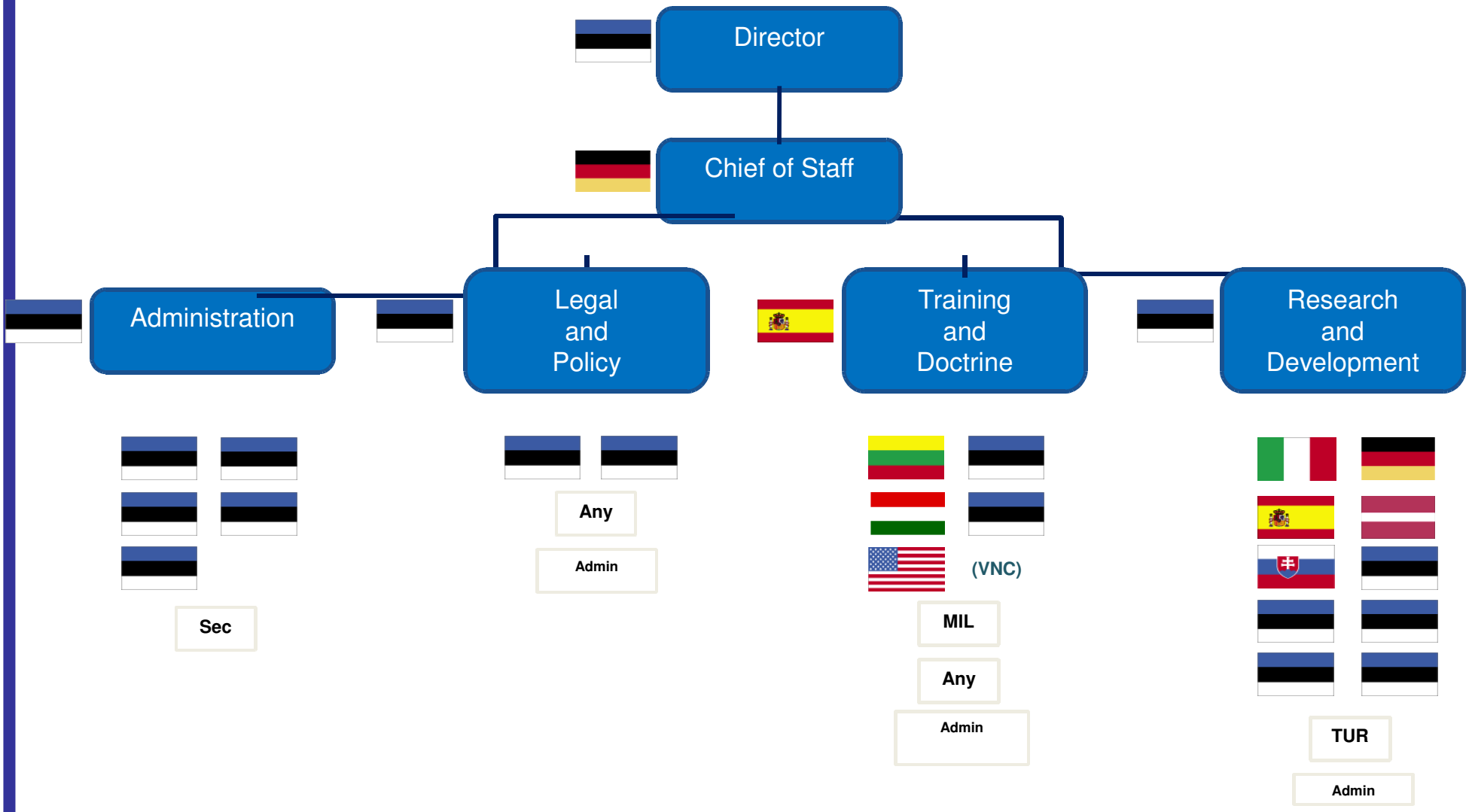
Mission: to enhance the cooperative cyber defence capability of NATO.

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 C3 AGENCY
NATO Consultation, Command and Control Agency
Agence OTAN de consultation, de commandement et de contrôle

Geir HALLINGSTAD
Principal Scientist
Cyber Defence and Assured Infomation 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**

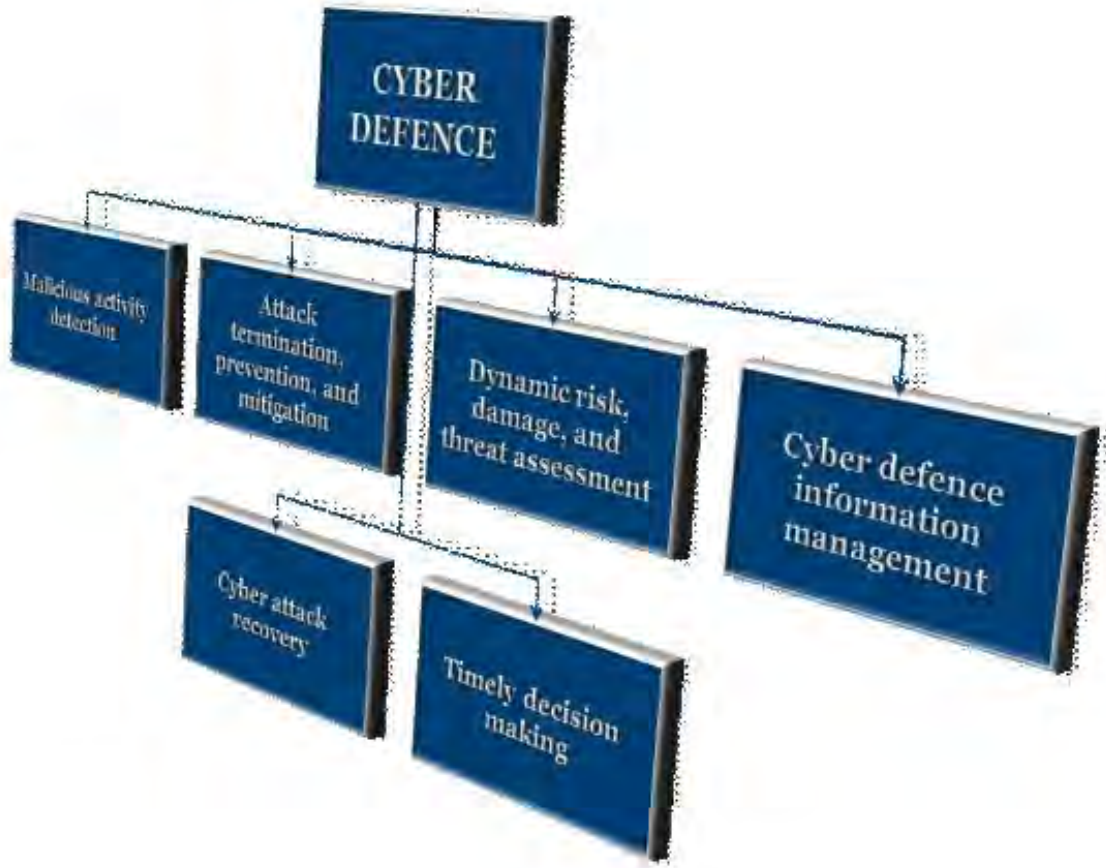
NATO
UNCLASSIFIED

Cyber Defence Capability Framework

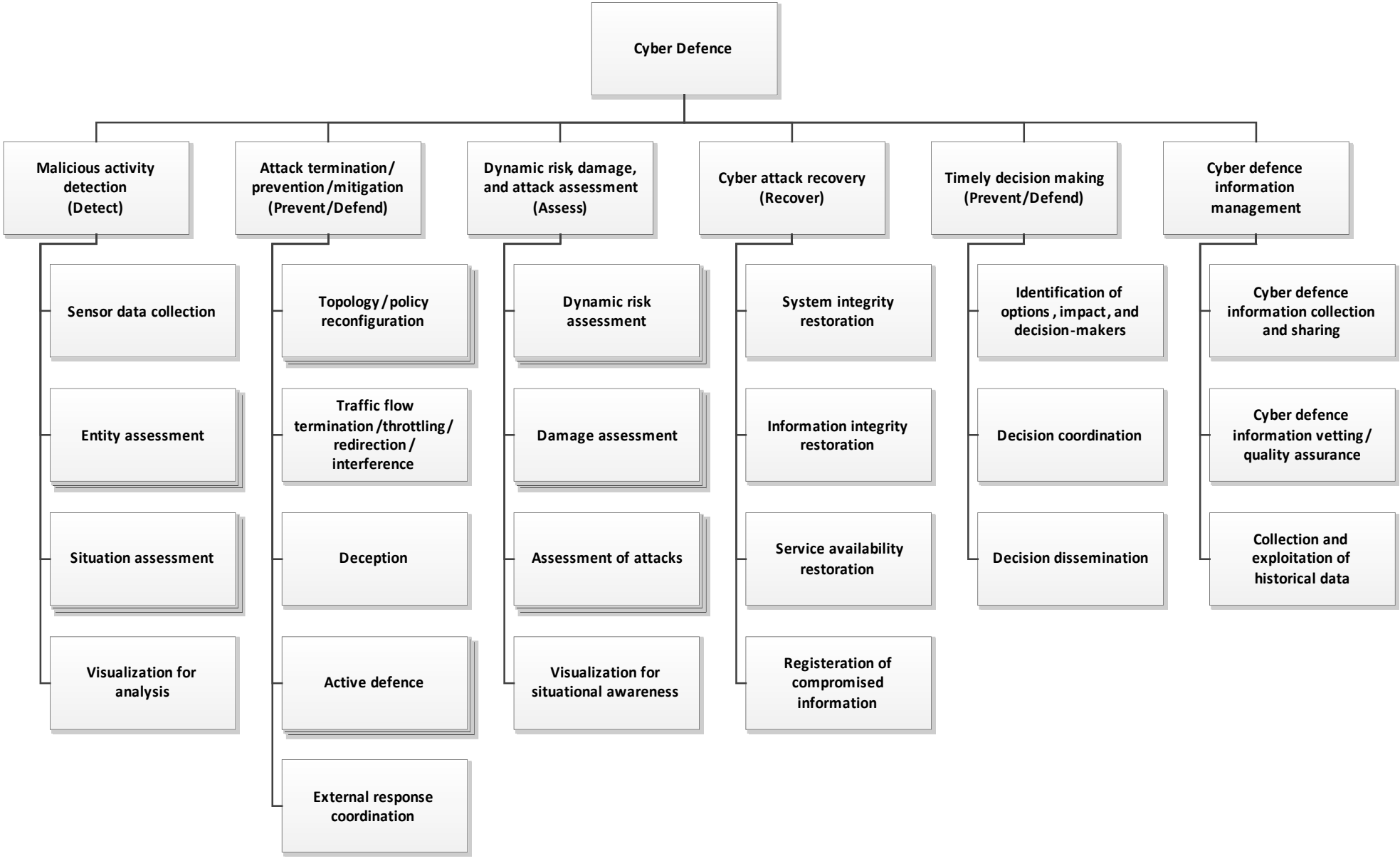
- **Objectives**
  - Establish the scope of cyber defence and the capabilities that are needed for a sound overall cyber defence capability
  - Provide a common taxonomy for more efficient discussion and coordination of cyber defence activities
  - Provide a framework for multinational cooperation on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

What is the Capability Breakdown

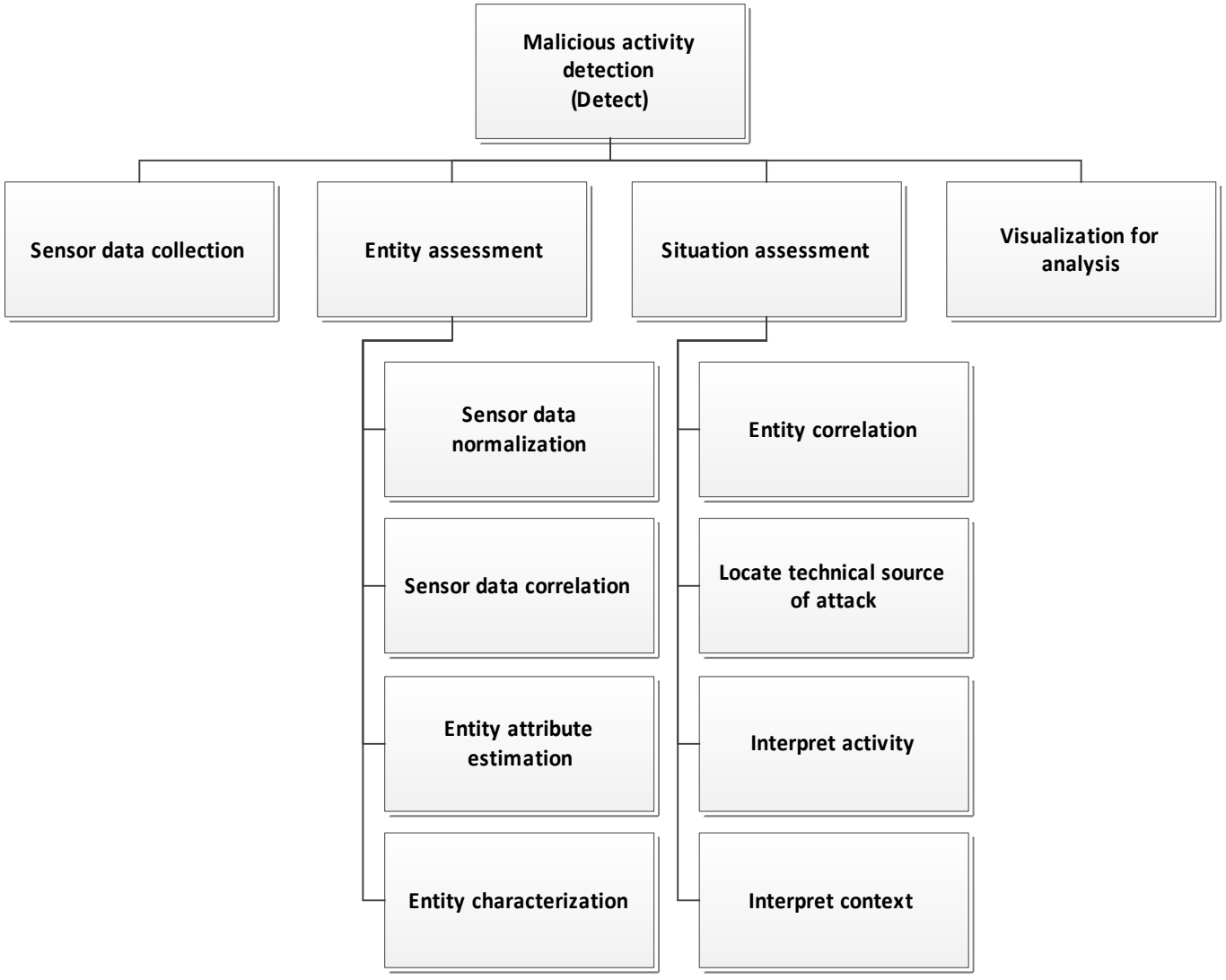
- **Capability**
  - The power/ability to do something
- **Hierarchical**
  - Structured capability breakdown
- **Does not address**
  - Processes; the order in which capabilities are used
  - Organization; who does what



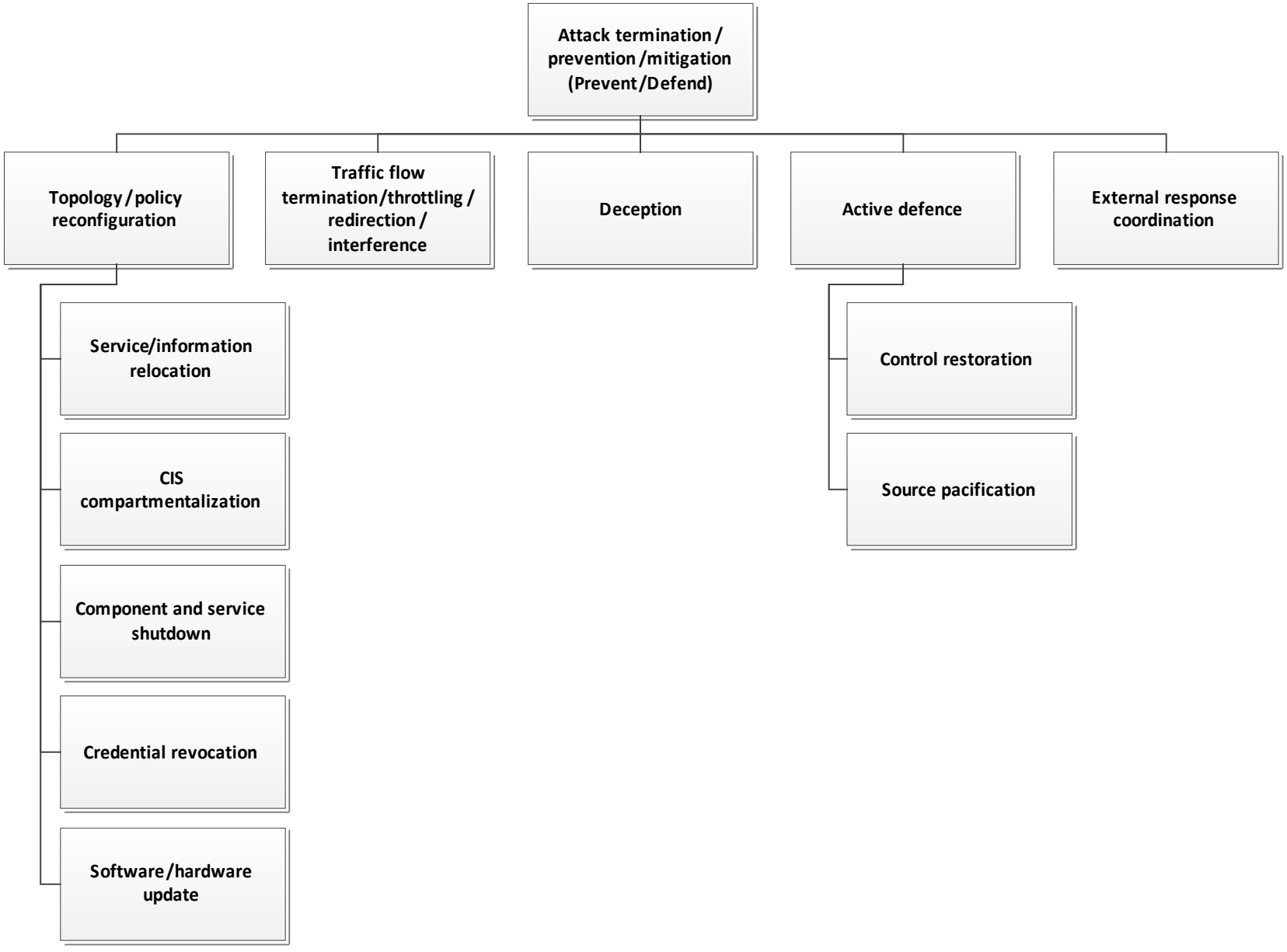
Cyber Defence Capability Breakdown



Malicious Activity Detection

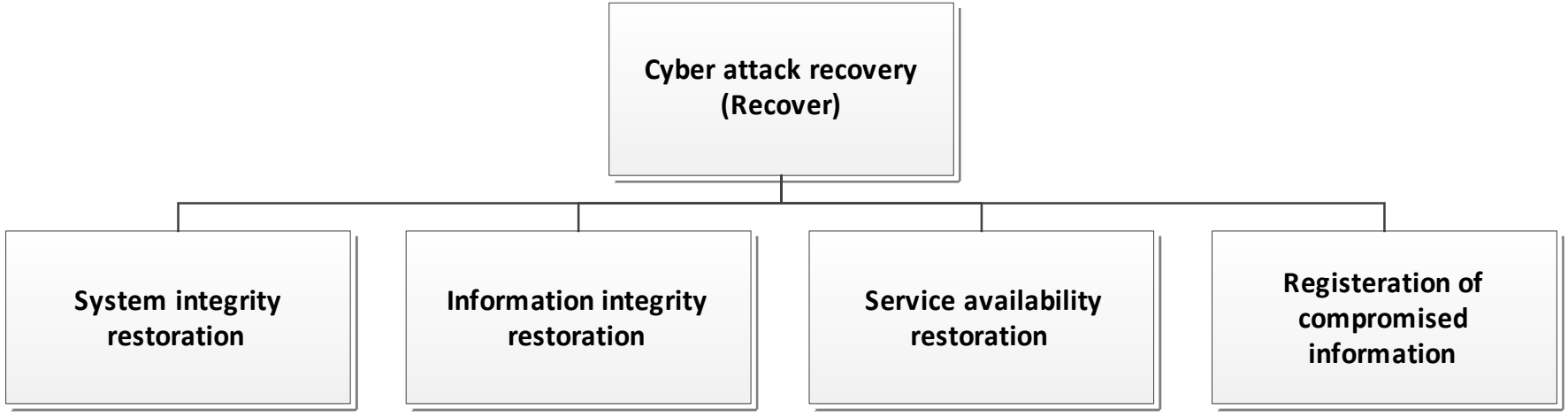


Attack termination, prevention, mitigation

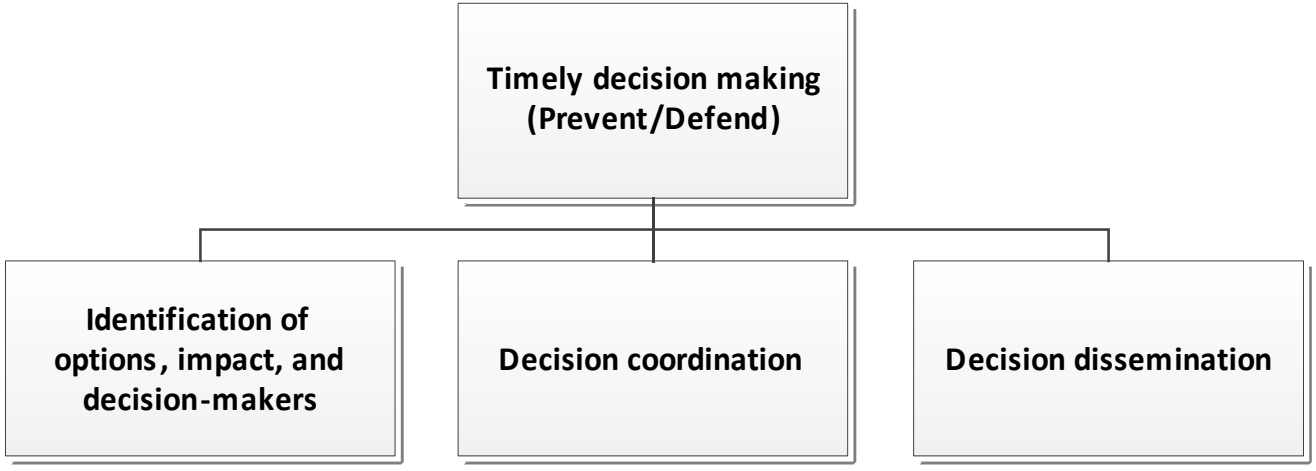


Dynamic Risk, Damage, and Threat Assessment

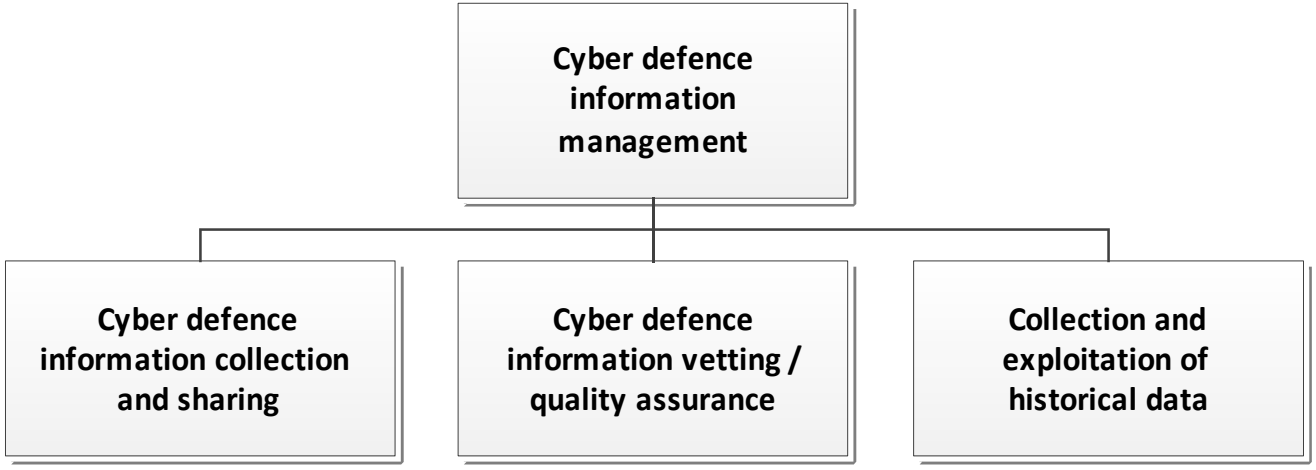
Cyber Attack Recovery



Timely Decision Making



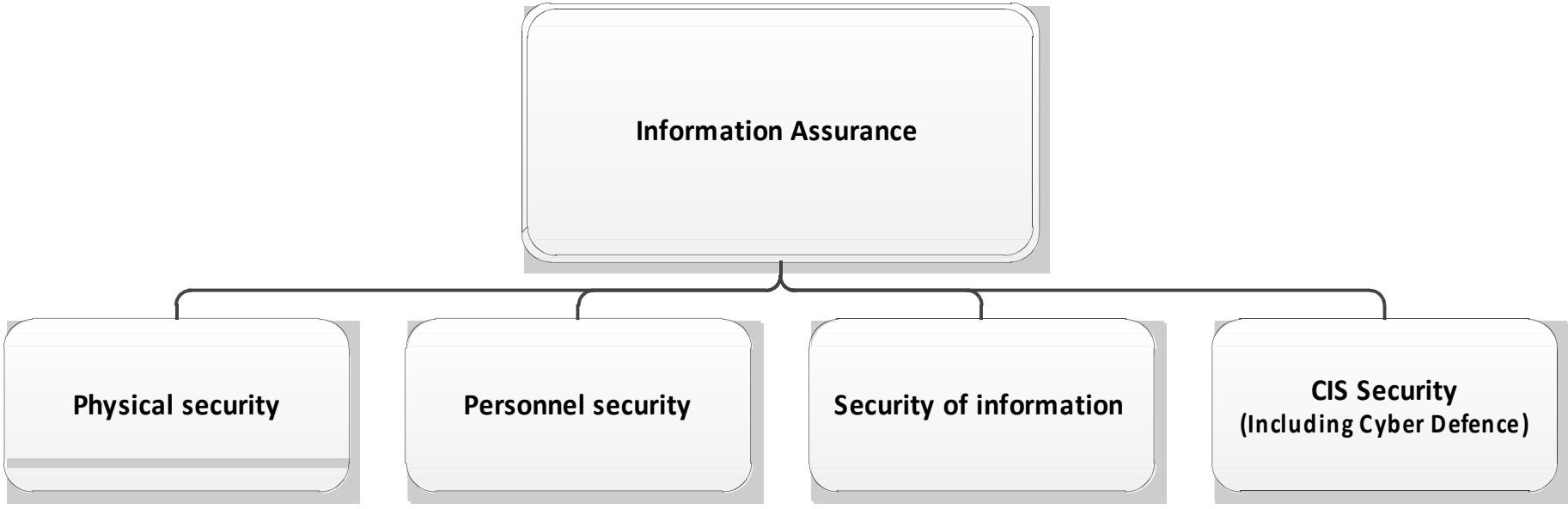
Cyber Defence Information Management



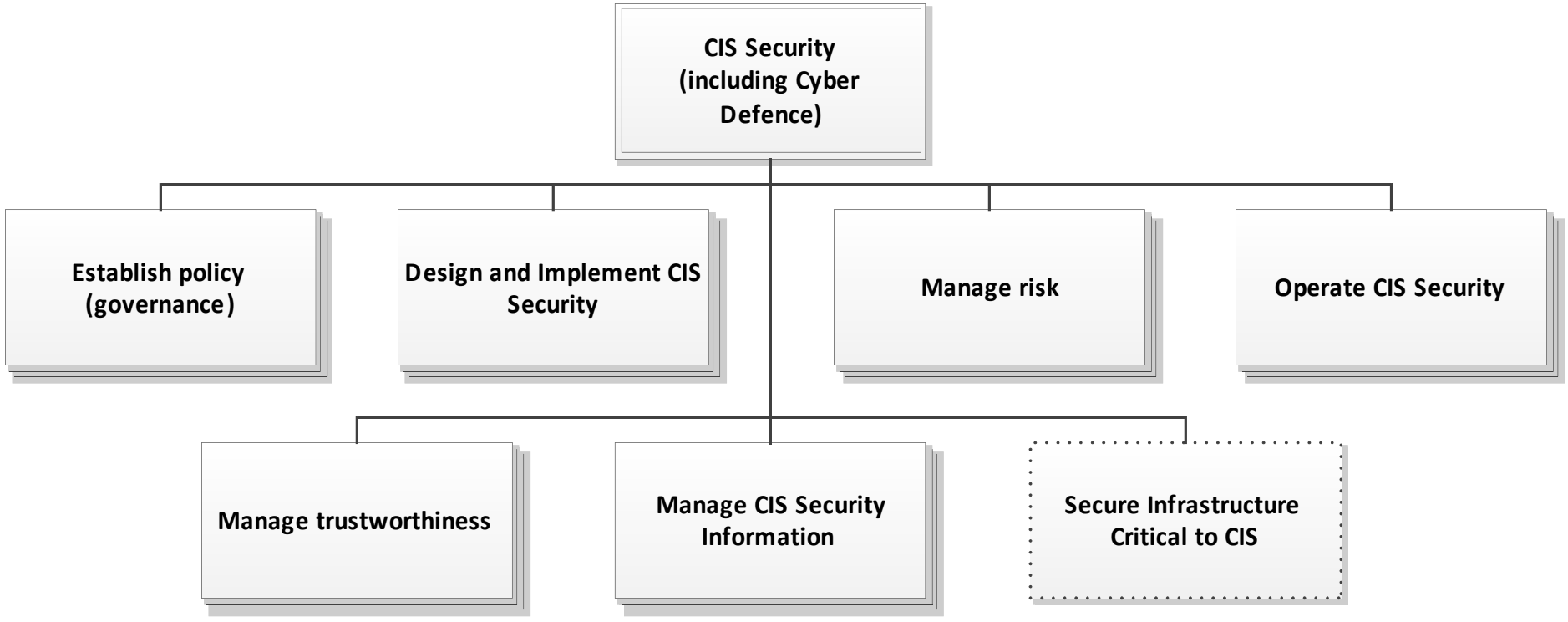
Cyber Defence User Applications

- 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

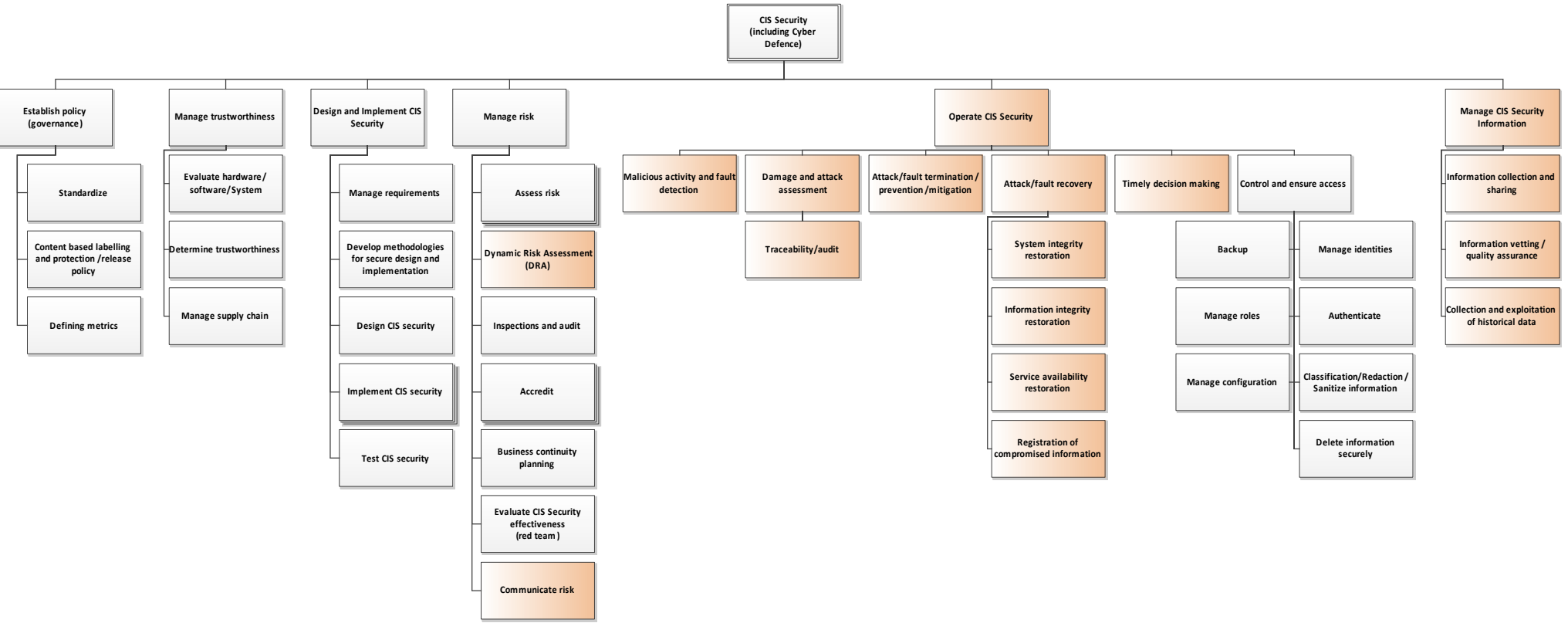


CIS Security (including Cyber Defence) Capability Breakdown



Work in progress …

Cyber Defence as part of CIS Security



Work in progress …

Miért jó ez nekünk?

- Egységes keretrendszert ad az események kezeléséhez

- Le tudja csökkenteni az improvizatív szakaszokat

- Rendszerezetté teszi a felkészülést az esetleges támadásokra, rendkívüli eseményekre

Az elkészült anyagok hozzáférhetõk:

ISACA®
Serving IT Governance Professionals

Kik használják a tudásközpont eredményeit?

ISACA®
Serving IT Governance Professionals

Ki NEM használja jelenleg a tudásközpont eredményeit?

Magyarország!

Kérdések?...

laszlo.biro@samunet.hu

ISACA®
Serving IT Governance Professionals

Thank you for your patience.

Köszönöm a türelmet!

ISACA®
Serving IT Governance Professionals