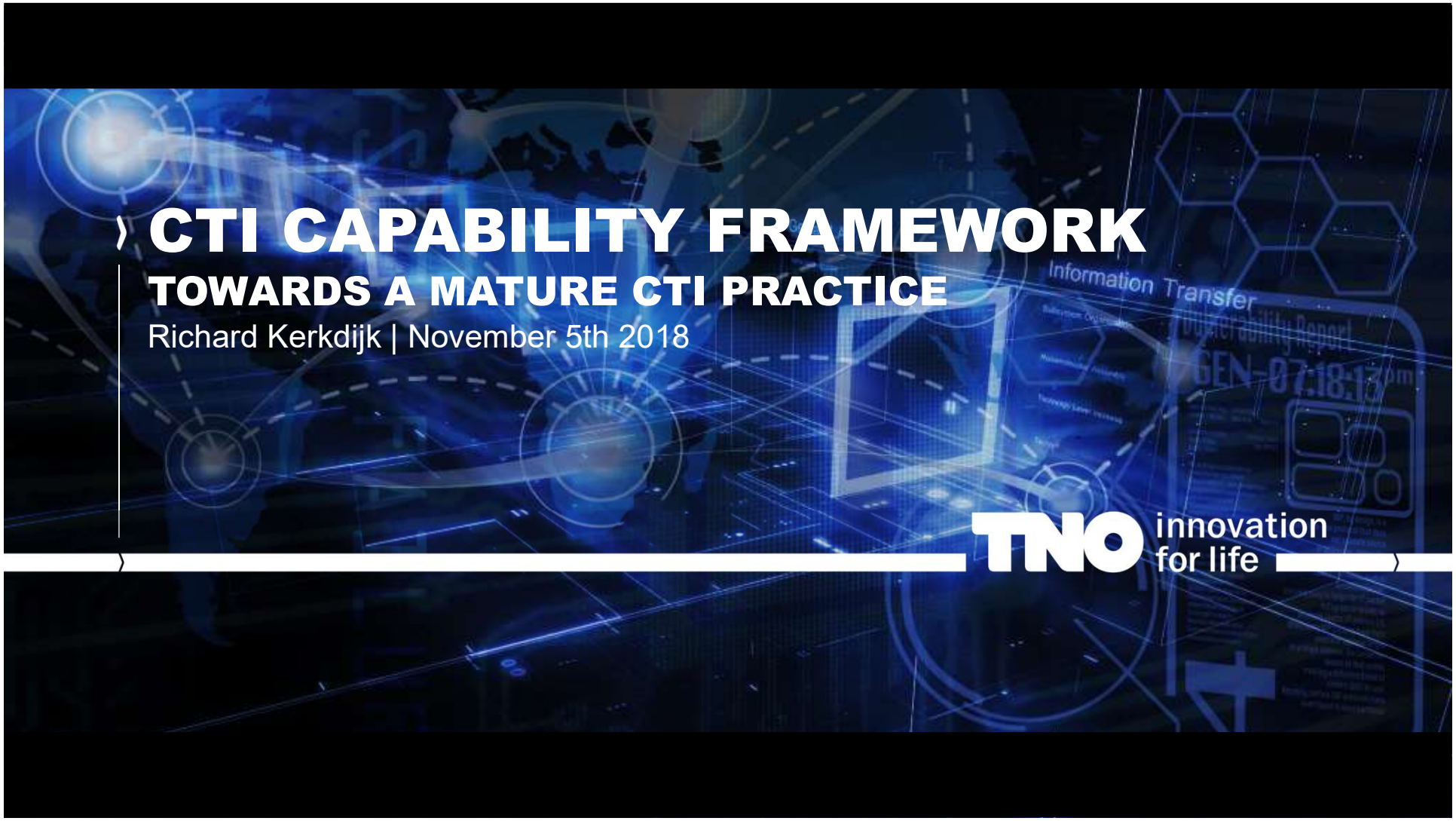
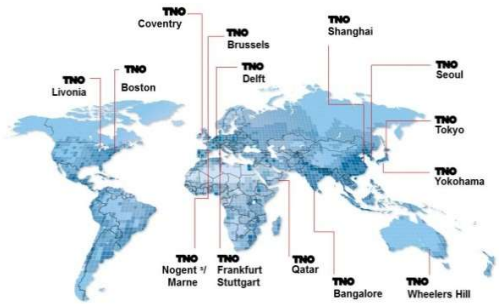


CTI CAPABILITY FRAMEWORK

TOWARDS A MATURE CTI PRACTICE

Richard Kerkdijk | November 5th 2018

A WORD ABOUT TNO



- Dutch **innovation and advisory** body, founded by law in 1932 and currently comprising some 2800 professionals
- Active in many fields (a.o. healthcare, automotive, defence, energy and ICT), not-for-profit and **independent** of public & private interests

Cyber Security team (~45 FTE)

(focus areas)

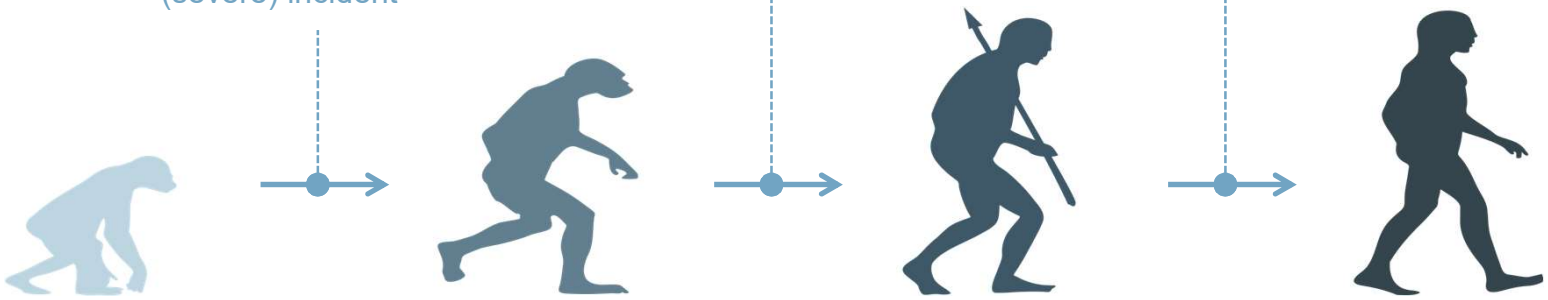
- **Monitoring & Detection**
- **Automated Security**
- **Transaction Security**

key partners

- Dutch government
- NCSC
- MoD/ Defence industry (NL)
- Financials (NL)
- Telcos (Europe)

EVOLUTION OF RESILIENCE STRATEGIES

often induced by
(severe) incident



Traditional prevention
put up walls and hope for the best

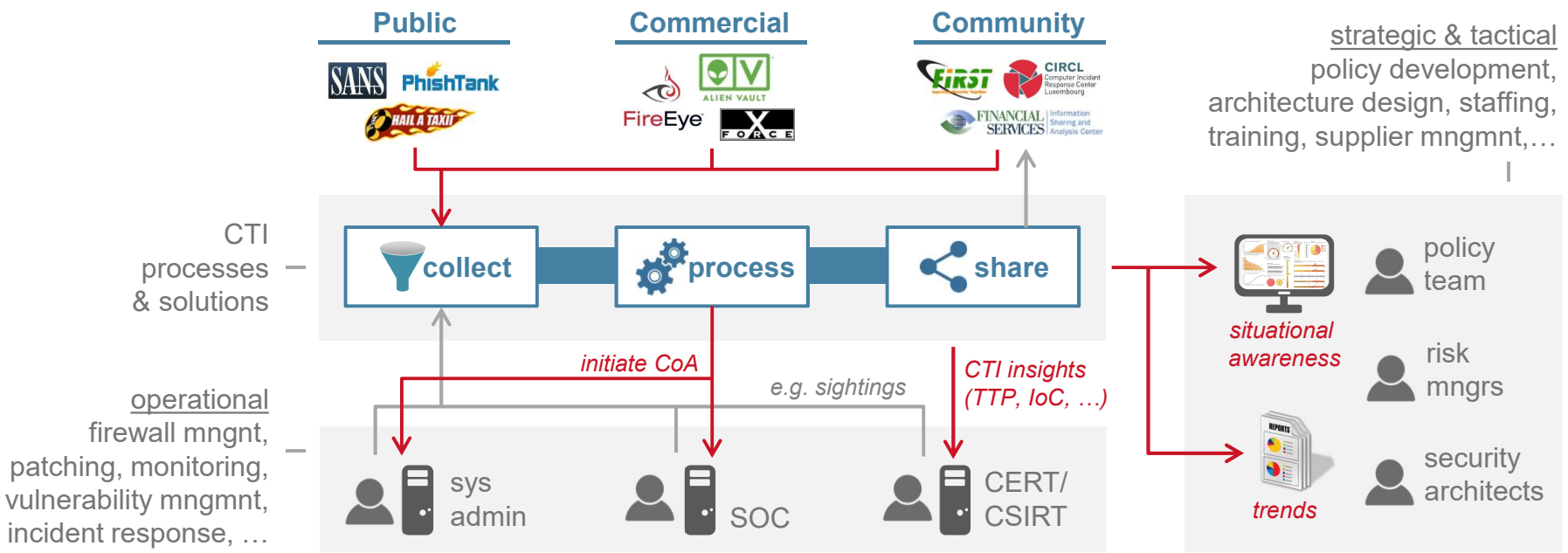
Monitoring & response construct
detect (potential) attacks and limit damage

Threat intelligence capabilities
anticipate and take proactive precautions

Autonomous response & recovery
reduce dependency on human operation

focus of this presentation

THE CTI PLAYING FIELD

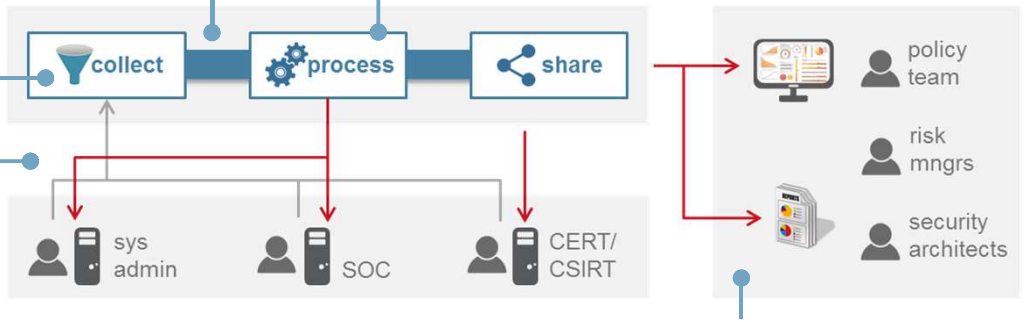


AN AREA THAT NEEDS MATURING

limited **resourcing** – duties usually reside in CSIRT

ad hoc workflows – relies on expertise of individuals

scattering of threat information – much resides in mailboxes

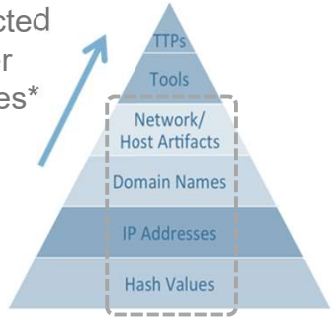


little **automation** – e.g. exchange of threat information via e-mail

underdeveloped – strong emphasis on operational processing

* Pyramid of Pain published by David Bianco

"pain" inflicted on cyber adversaries*



focus of activities

*present efforts largely revolve around **indicators** – but the real value lies in tactical intelligence!*

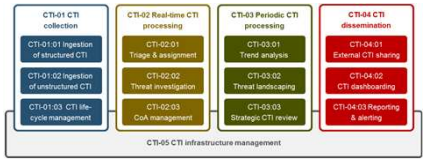
BUT WHAT CONSTITUTES “MATURE”?

CSIRT Handbook by CERT/CC

- Description of typical CSIRT services (2003), a.o. adopted by ENISA.
- **No clear definition** of CTI related services

revision?

CTI Capability Framework

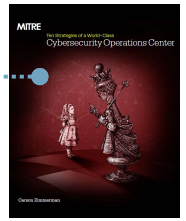


ABN·AMRO ING Rabobank TNO

- Intended as **tangible and contemporary** foundation for maturing CTI provisions
- Developed in collaboration with major Dutch financials.

inspiration

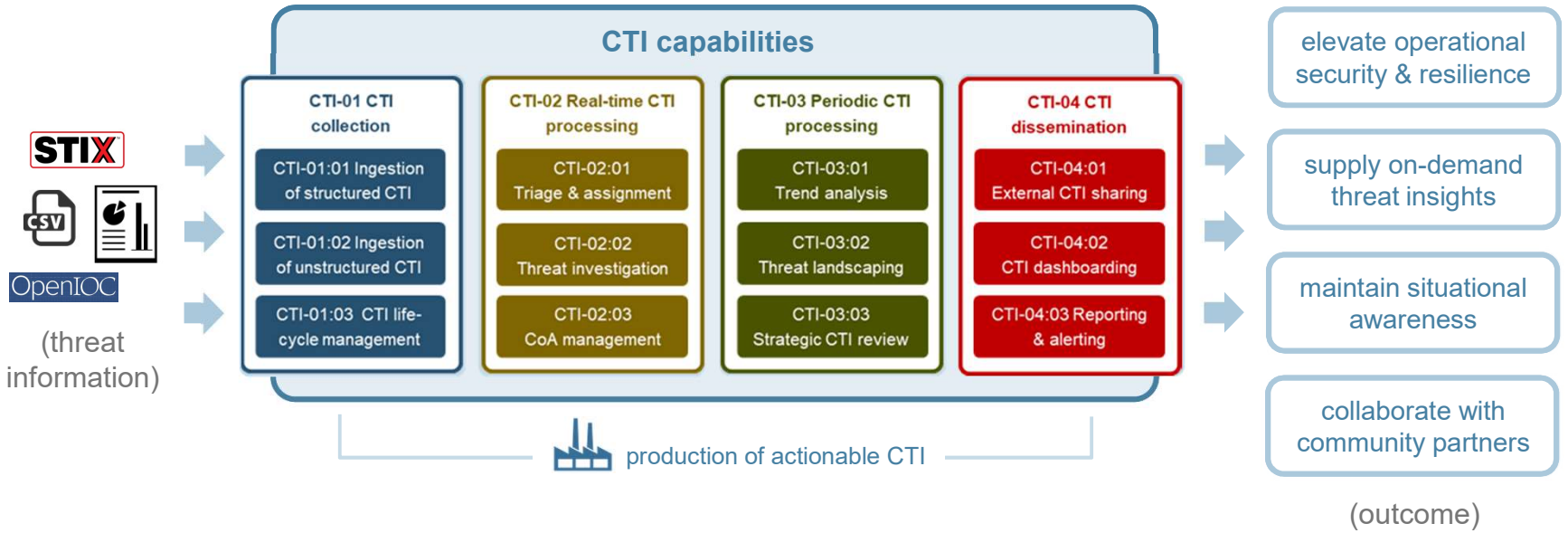
MITRE’s SOC Capabilities



Carson Zimmerman, “Ten Strategies of a World-Class Cyber Security Operations Center”

- Modern perspective (2014), includes “intel & trending”
- **Not particularly focused** on CTI - much embedded in broader SOC capability

DEFINING CTI CAPABILITIES



ELEVATE OPERATIONAL SECURITY

threat indicators

production of actionable CTI

- monitor (SIEM, IDS)
- block (firewall, ACL)
- hunt (data lake)

(typical setup)

CTI-01:01 Ingestion of structured CTI

- ❑ establish indicator feeds
- ❑ pre-process for analysis

CTI-01:03 CTI life-cycle management

- ❑ CTI source & data maintenance

CTI-02:01 Triage & assignment

- ❑ select CoA
  - automated
  - playbook
  - expert

(fast throughput)

CTI-02:02 Threat investigation

- ❑ assess threat & possible mitigations
- ❑ select action
  - CoA
  - monitor
- ❑ standardise for fast triage

CTI-02:03 CoA management

- ❑ prepare CoA *(e.g. signature)*
- ❑ initiate CoA
  - API
  - ticket
- ❑ monitor CoA establishment

SUPPLY ON-DEMAND THREAT INSIGHTS

actors, TTP, campaigns….

production of actionable CTI

Q

specific threat insights

CERT/CSIRT

(typical scenario)

CTI-01:01 Ingestion of structured CTI

- establish tactical feeds
- pre-process for analysis

CTI-01:02 Ingestion of unstructured CTI

- acquire threat reports/ mailings
- abstract machine readable threat information

CTI-02:02 Threat investigation

- analyse & correlate threat information

archive in structured repository

CTI-04:02 CTI dashboarding

- self-service portal
  - current threats
  - actor analysis
  - …

(align with needs of target audiences)

MAINTAIN SITUATIONAL AWARENESS

threat information

production of actionable CTI

trends

Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware		→
2. Web based attacks		→
3. Web application attacks		→
4. Denial of service		↑
5. Botnets		↓
6. Phishing		↑

(example)

from: ENISA Threat Landscape Report 2016

CTI-03:01 Trend analysis

- ❑ analyse threat info collected over time
- ❑ ID structural changes, e.g. in attacker MO

(often fed by trigger)

CTI-03:02 Threat landscaping

- ❑ assess effects of CTI trends and events
- ❑ create prioritized list of cyber threats

CTI-03:03 Strategic CTI review

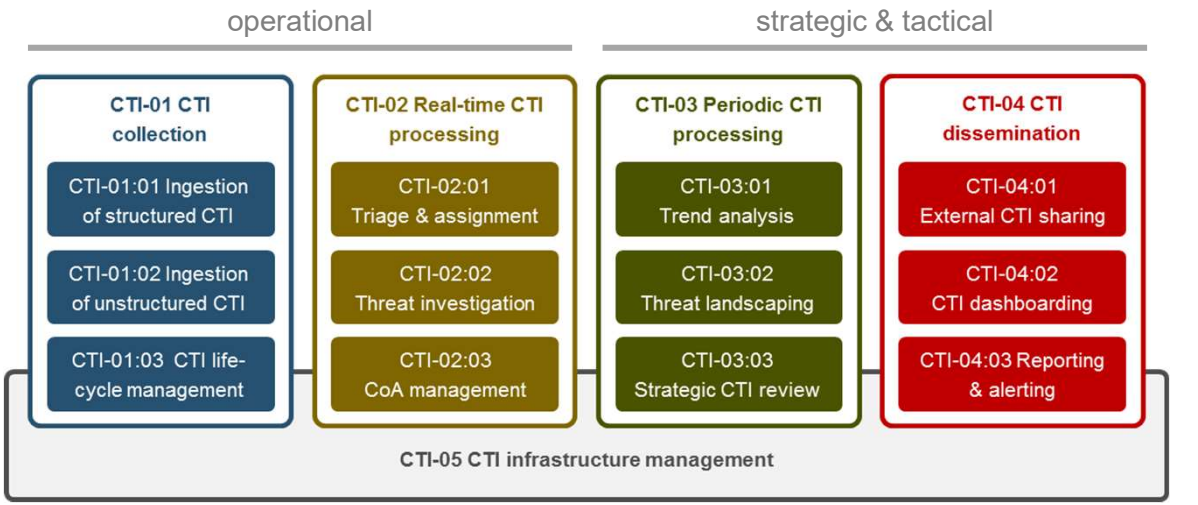
- ❑ ID threats/ trends for which organisation is not prepared
- ❑ assess causes/ shortcomings
- ❑ raise with security leaders

CTI-04:03 Reporting & alerting

- ❑ ID stakeholders & their needs
- ❑ develop reporting products/ formats
- ❑ create and distribute reports

CTI CAPABILITY FRAMEWORK

each documented in detail – definition, context, guidance



CTI-01:01 Ingestion of structured CTI
Definition The ability to consume, normalise and enrich machine readable threat information and feed it to the organisation's CTI repository in a fully automated fashion.
Context The purpose of this capability is to ingest (periodic or ongoing) feeds of structured CTI into the organisation's CTI repository. The term "structured" refers to threat information that comes in standardised, "machine readable" formats (e.g. STIX, IODEF or OpenIOC) and can thus be processed fully automatically. Indicators of Compromise (IoCs) are a typical example, but contemporary standards such as STIX also accommodate structured representation of threat actors, campaigns, attacker methods and Courses of Action.
Guidance • In essence, ingestion of structured CTI involves the establishment of periodic and/or ongoing feeds of threat information towards a CTI collection device. For external sources this will often require a subscription or

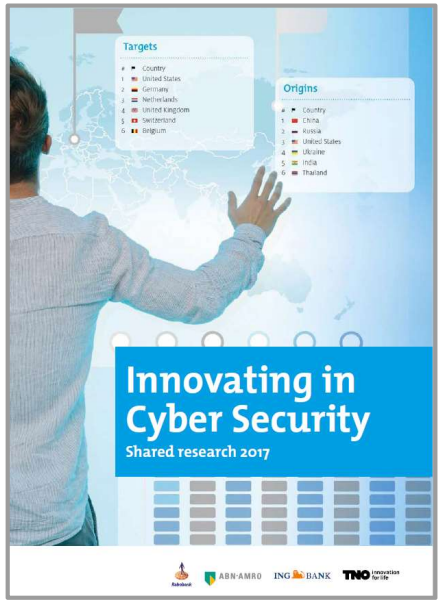
- 12 **practice oriented** capabilities for establishing a CTI practice
- Explicitly **detached** from security team demarcations (SOC, CERT…)
- Work ongoing to transform into **ENISA guideline**

TAKE AWAYS

- We see a need for a **CTI capability framework** that can serve as a foundation for establishing a mature CTI practice.
- The value of such a framework extends beyond the parties that first developed it. A body such as ENISA could bring (its own iteration of) the framework to a broader **European audience**.
- Not every organization will need (or be able) to develop all capabilities encompassed in the proposed framework – a **balanced selection** can also be appropriate.

THANK YOU & FURTHER READING

Richard Kerkdijk
+31 6 2290 64 64
richard.kerkdijk@tno.nl



https://www.tno.nl/media/9419/innovating-in-cyber-security.pdf