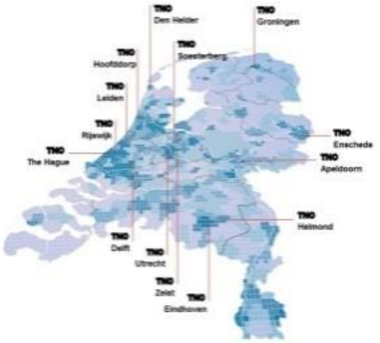
CYBER THREAT INTELLIGENCE

INNOVATING TOWARDS A MATURE PRACTICE

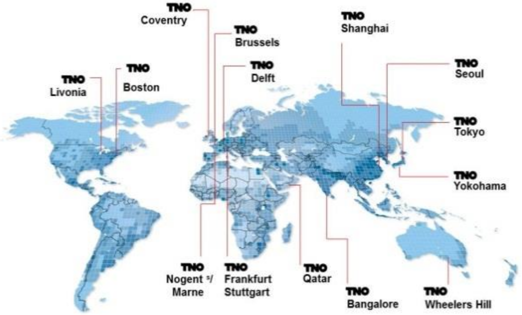
Richard Kerkdijk | January 19th 2017

TNO innovation for life

A WORD ABOUT TNO

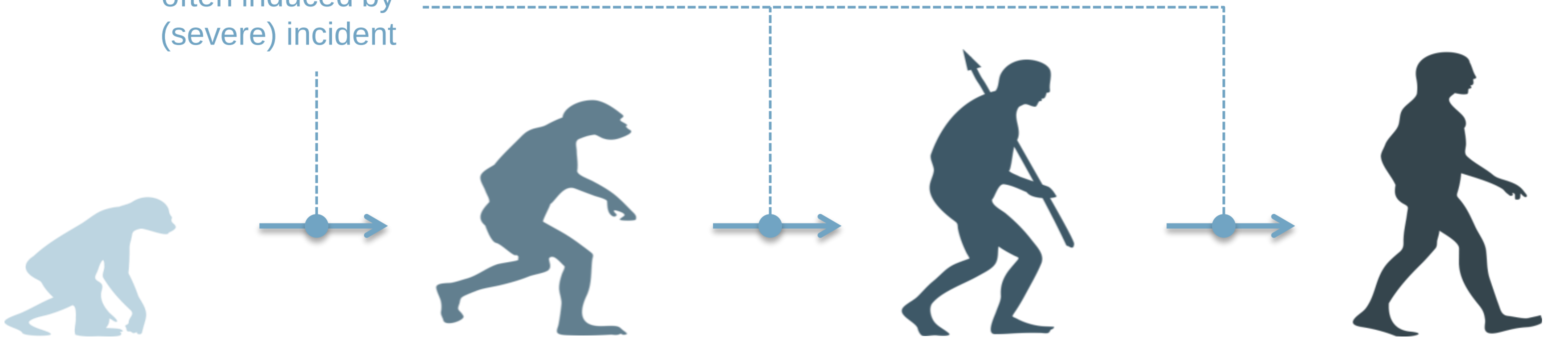


- Dutch **innovation and advisory** body, founded by law in 1932 and currently comprising some 2800 professionals
- Active in many fields (a.o. healthcare, automotive, defence, energy and ICT), not-for-profit and **independent** of public & private interests
- Very active in the field of **cyber security** – R&D, contract research, consulting
- Variety of customers - government, MoD, telcos, financials, energy companies, …



EVOLUTION OF RESILIENCE STRATEGIES

often induced by
(severe) incident



Traditional prevention
put up walls and
hope for the best

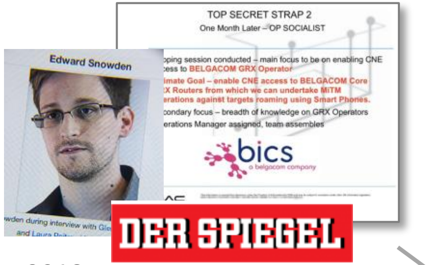
Monitoring & response construct
detect (potential) attacks
and limit damage

Threat intelligence capabilities
anticipate and take
proactive precautions

Autonomous response & recovery
reduce dependency
on human operation

focus of this presentation

SO WHAT IS THREAT INTELLIGENCE?



TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

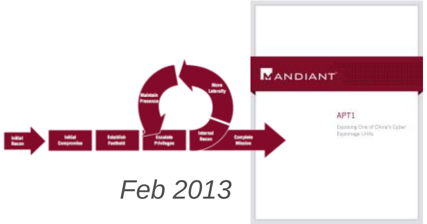
oping session conducted – main focus to be on enabling CNE cess to BELGACOM GRX Operator

imate Goal – enable CNE access to BELGACOM Core X Routers from which we can undertake MiTM erations against targets roaming using Smart Phones.

condary focus – breadth of knowledge on GRX Operators

erations Manager assigned, team assembles

Sep 2013



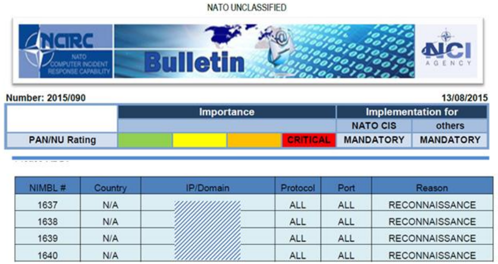
MANDIANT

APT1

Exposing One of China's Cyber Espionage Units

Feb 2013

threat actors, attacker campaigns, attacker techniques (TTP), Indicators of Compromise, Courses of Action….



NATO UNCLASSIFIED

NCIRC
NATO COMPUTER INCIDENT RESPONSE CAPABILITY
Bulletin
NCI AGENCY

Number: 2015/090

13/08/2015

	Importance				Implementation for	
					NATO CIS	others
PAN/NU Rating	🟩	🟨	🟧	CRITICAL	MANDATORY	MANDATORY

NIMBL #	Country	IP/Domain	Protocol	Port	Reason
1637	N/A	[redacted]	ALL	ALL	RECONNAISSANCE
1638	N/A	[redacted]	ALL	ALL	RECONNAISSANCE
1639	N/A	[redacted]	ALL	ALL	RECONNAISSANCE
1640	N/A	[redacted]	ALL	ALL	RECONNAISSANCE

NIMBL = NCIRC Identified Malware Black List

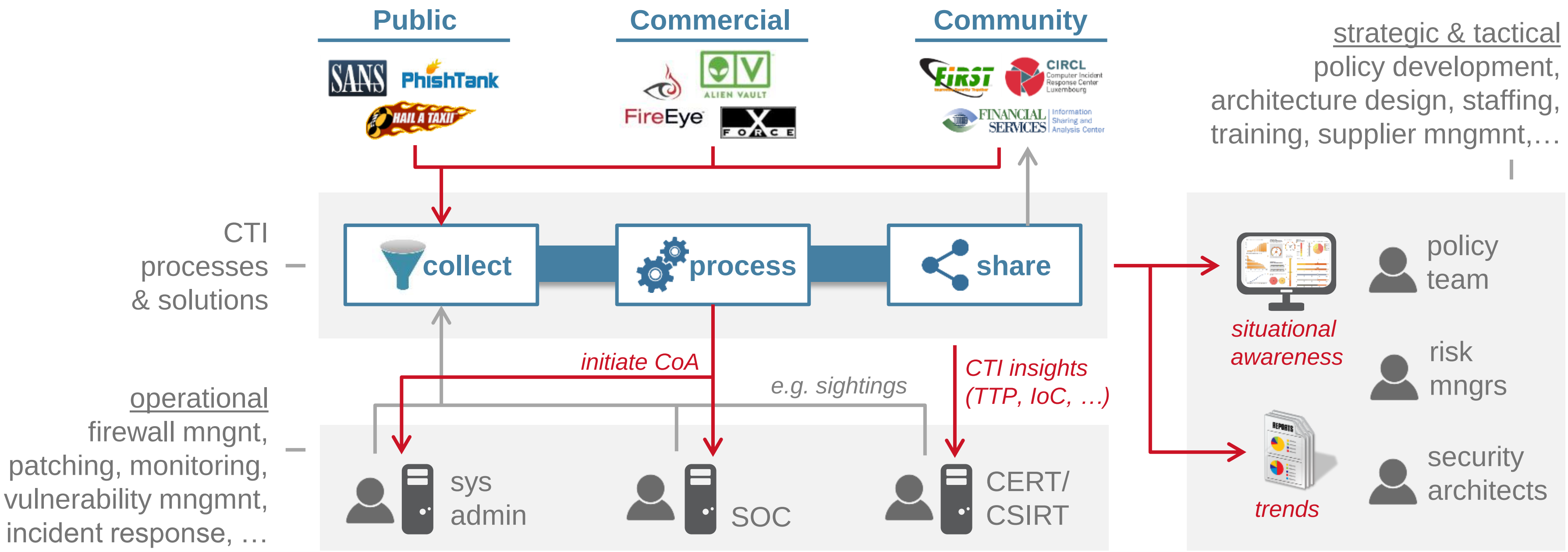
Cybersecuritybeeld Nederland

CSBN 2015

“Cryptoware and other ransomware constitute preferred business model for cyber criminals”

Nov 2015

THE CTI PLAYING FIELD



Public

Commercial

Community

SANS
PhishTank
HAIL A TAXII
FireEye
ALIEN VAULT
X FORCE
FIRST
CIRCL Computer Incident Response Center Luxembourg
FINANCIAL SERVICES Information Sharing and Analysis Center

CTI processes & solutions

collect

process

share

initiate CoA

e.g. sightings

CTI insights (TTP, IoC, …)

operational

firewall mngnt, patching, monitoring, vulnerability mngmnt, incident response, …

sys admin

SOC

CERT/ CSIRT

strategic & tactical

policy development, architecture design, staffing, training, supplier mngmnt,…

situational awareness

trends

policy team

risk mngrs

security architects

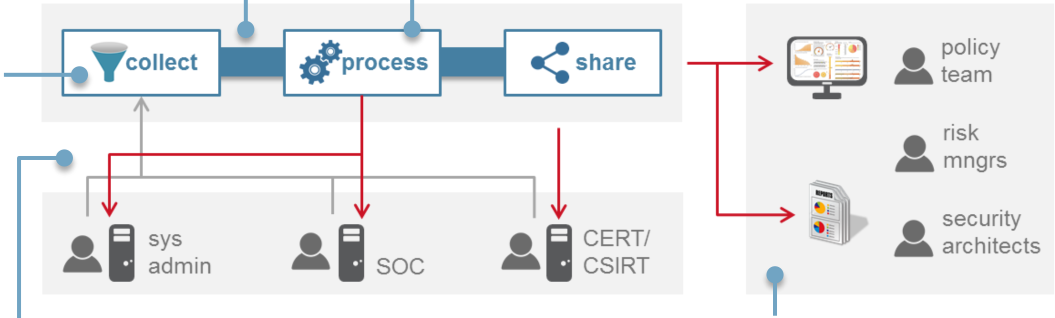
AN AREA THAT NEEDS MATURING

** Pyramid of Pain published by David Bianco*

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

ad hoc workflows – relies on expertise of individuals

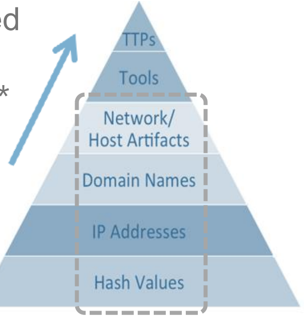
scattering of threat information – much resides in mailboxes



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

underdeveloped – strong emphasis on operational processing

“pain” inflicted on cyber adversaries*

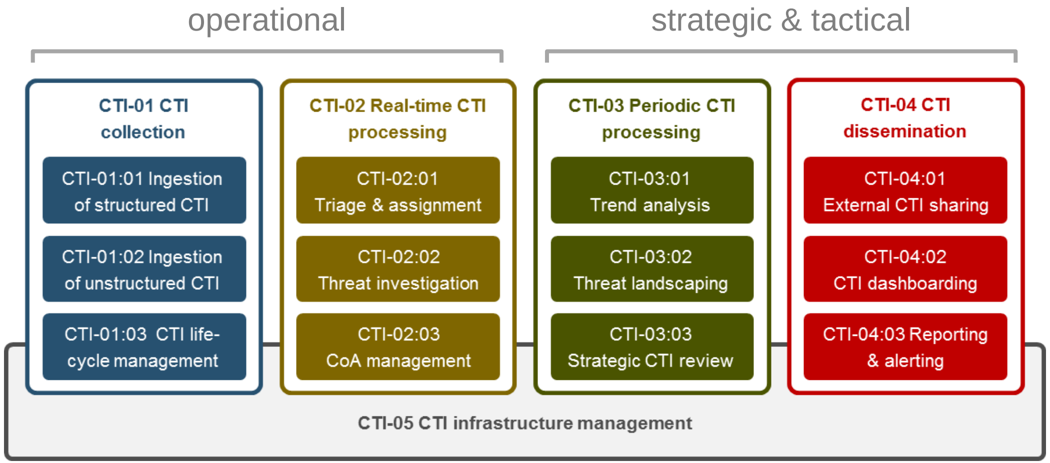


focus of activities

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

CTI CAPABILITY FRAMEWORK

<u>Note</u>: TNO and the involved financials are preparing an article on the CTI capability framework which is set to be published this April.



operational

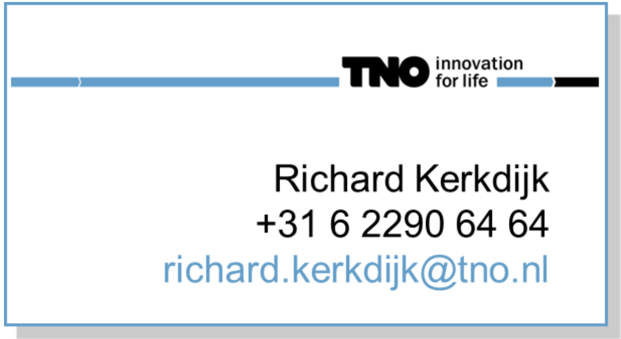
strategic & tactical

CTI-01 CTI collection	CTI-02 Real-time CTI processing	CTI-03 Periodic CTI processing	CTI-04 CTI dissemination
CTI-01:01 Ingestion of structured CTI	CTI-02:01 Triage & assignment	CTI-03:01 Trend analysis	CTI-04:01 External CTI sharing
CTI-01:02 Ingestion of unstructured CTI	CTI-02:02 Threat investigation	CTI-03:02 Threat landscaping	CTI-04:02 CTI dashboarding
CTI-01:03 CTI life-cycle management	CTI-02:03 CoA management	CTI-03:03 Strategic CTI review	CTI-04:03 Reporting & alerting

CTI-05 CTI infrastructure management

- Demarcates **target situation** – foundation for maturing CTI provisions
- Developed because **traditional** CSIRT service descriptions (e.g. CERT/CC) do not (fully) capture CTI working area

THANK YOU



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