



Be prepared against today's threats with TIBER

 Rob Wassink (DNB) &  Vincent Waart (EY)

ISACA Square Table 28 October 2020

TIBER-NL: Background



02 januari 2020 15:01
Laatste update: 03 januari 2020 07:51



De Universiteit Maastricht (UM) heeft losgeld betaald aan de criminelen achter de gijzelsoftware die de universiteit al meer dan een week in zijn ban houdt, melden ingewijden aan [Observant](#), de onafhankelijke krant van de universiteit. Het zou hierbij gaan om een paar ton. Een woordvoerder van de universiteit wil het bericht niet aan NU.nl bevestigen, maar kan het ook niet ontkennen.



FINANCIAL

Equifax to pay customers \$380.5 million as part of final breach settlement



The judge's decision Monday represents the final approval of a settlement deal initially proposed in July. (Flickr)

TIBER-NL: Big new in the Netherlands

Menu **nrc.nl**

Hackers van DNB gaan beveiliging banken testen

De toezichthouder publiceert dinsdag een handleiding waarmee banken de tests kunnen organiseren.

Menno Sedee 14 november 2017 Leestijd 1 minuut



fd. Mijn nieuws 7+ Laatste nieuws Krant Dossiers Beurs Meer ▾

Joost Dobber 14 nov 17 Tekst Krant

ONDERNEMEN

DNB gaat proberen de banken te hacken

Een team onder de vlag van De Nederlandsche Bank (DNB) gaat de Nederlandse financiële infrastructuur hacken. Door geheime testaanvallen uit te voeren op banken, beursexploitanten en clearinghuizen hopen toezichthouder en de financiële sector gezamenlijk de digitale veiligheid te vergroten.

Volgen via mijn nieuws

- Banken
- Cybersecurity

De Telegraaf NIEUWS SPORT ENTERTAINMENT FINANCIEEL VROUW

NIEUWS

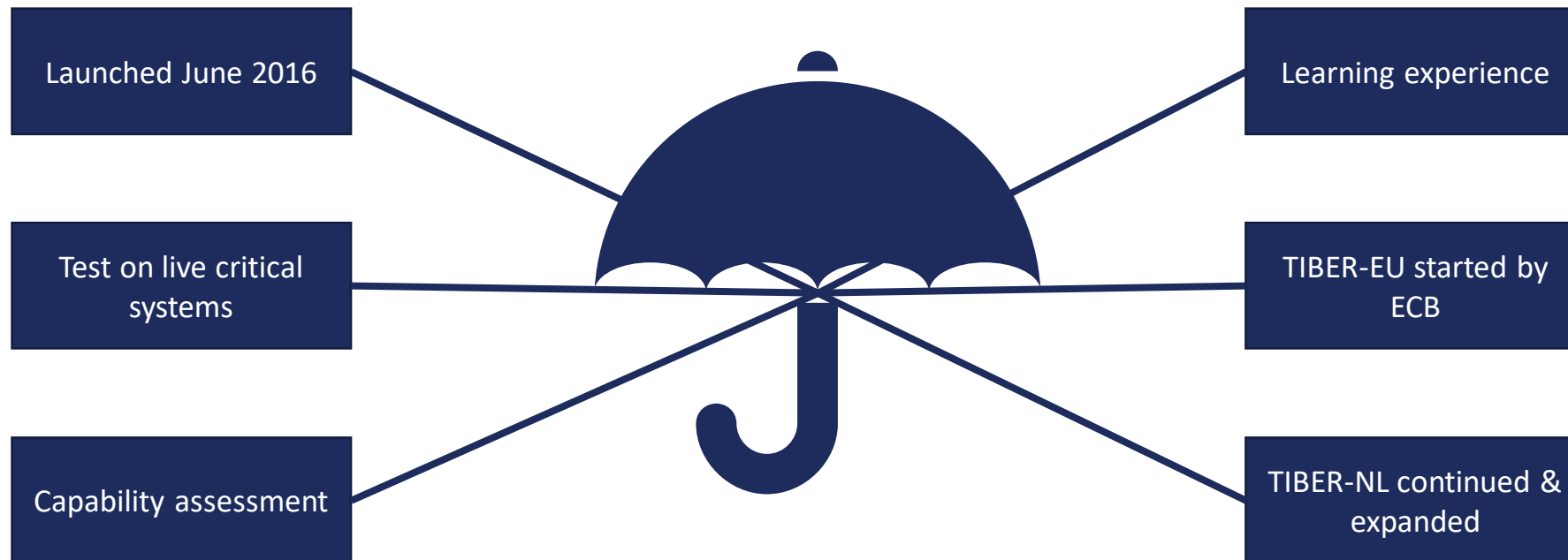
DNB test banken met aanval hackers

Door **DOOR RUBEN EG**
27 nov. 2015 in NIEUWS

f t e g



TIBER-NL: The making of



TIBER-NL: Participants from 2019 till 2021



Financial Core
Infrastructure (FCI)



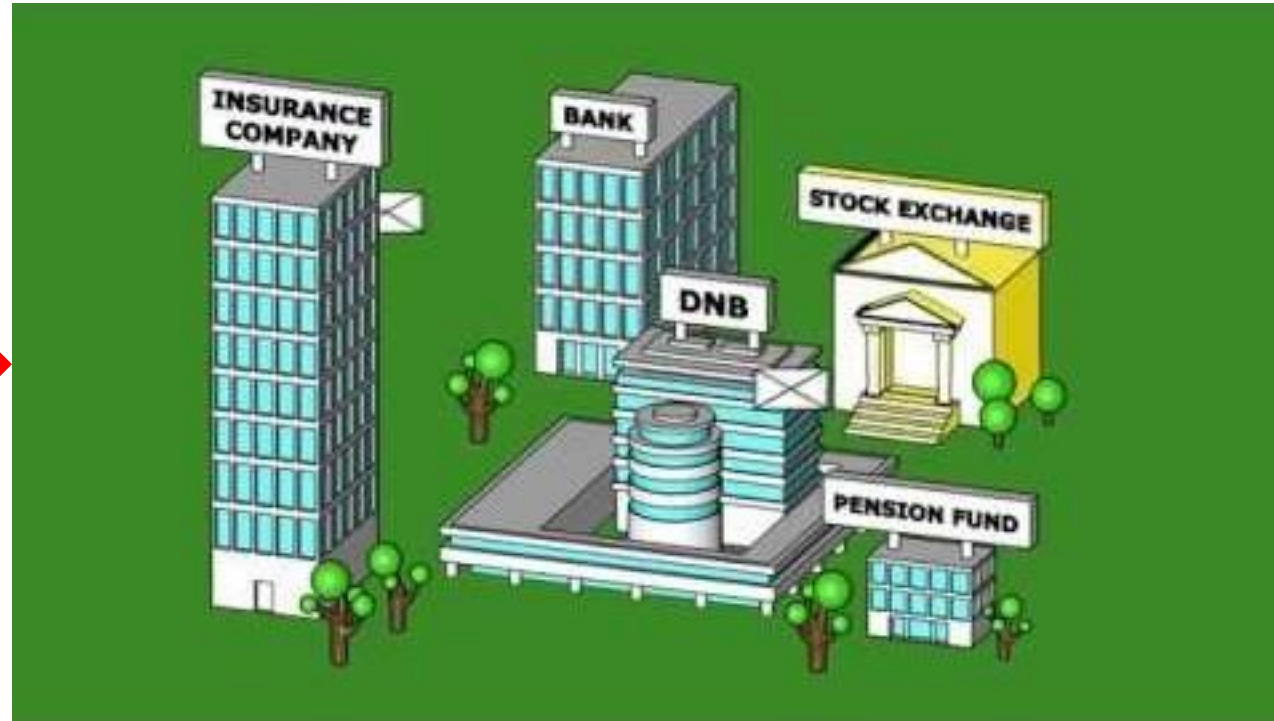
Pension Providers



Insurance Companies

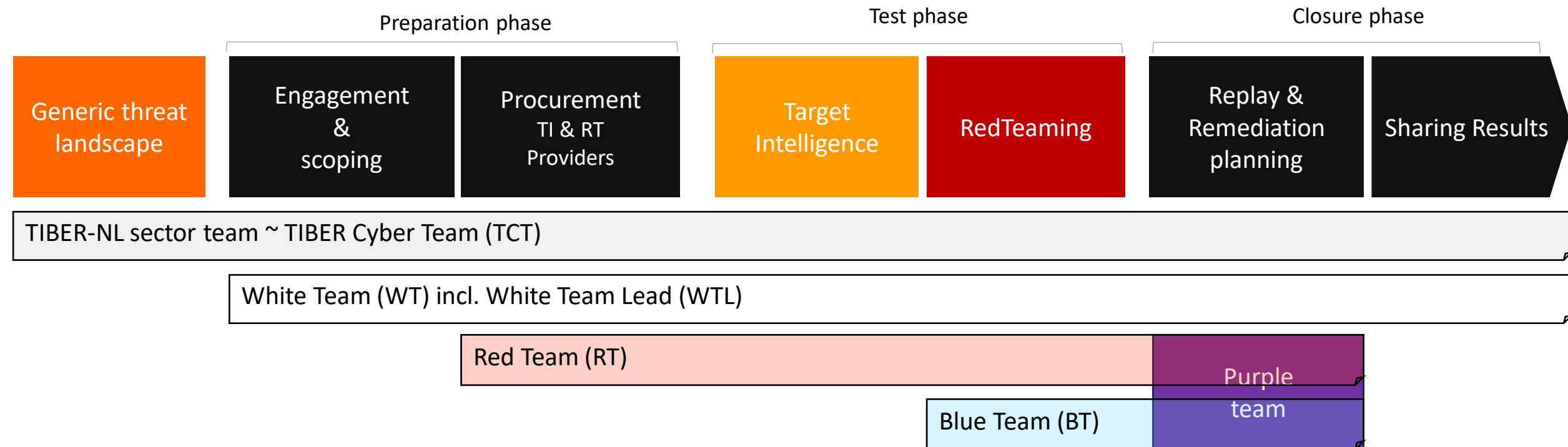
TIBER-NL: Introduction

PLAY VIDEO



Source: <https://www.youtube.com/watch?v=-dXf96mot2A>

TIBER-NL: Process



Cyber Kill Chain



Example attack: Maastricht University



1. Malicious Office files spread via email to targeted individuals



2. Workstations and Virtual Desktops infected with SDBBot malware



3. Manual spread over the network with Meterpreter to more Workstations and Virtual Desktops



4. Multiple Windows Servers compromised, likely via EternalBlue



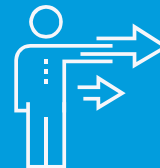
5. Compromised workstations used to run tools to explore environment and AD



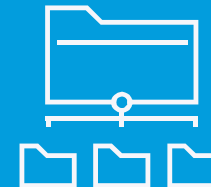
6. Meterpreter used on another server, Domain Admin credentials found



7. Domain Admin credentials used to login on Domain Controller



8. Preparations for deployment of ransomware and removal of McAfee



9. Domain Admin account used to deploy malware to servers



10. Ransomware encrypts the files on 267 servers

TIBER vs. Red Teaming

What?	Red Teaming	TIBER
Testing Cyber Resilience	✓	✓
Controlled environment	✓	✓
Realistic scenario's	✓	✓
'Carte Blanche' for attackers	✗	✓
Targets live systems	✗	✓
Sharing Results with community	✗	✓
International accreditation	✗	✓

“What would you hope to learn from a Red Teaming or TIBER assessment?”

TIBER-EU

TIBER-NL

TIBER-EU

TIBER-BE

TIBER-DK

TIBER-IE

TIBER-RO

TIBER-DE

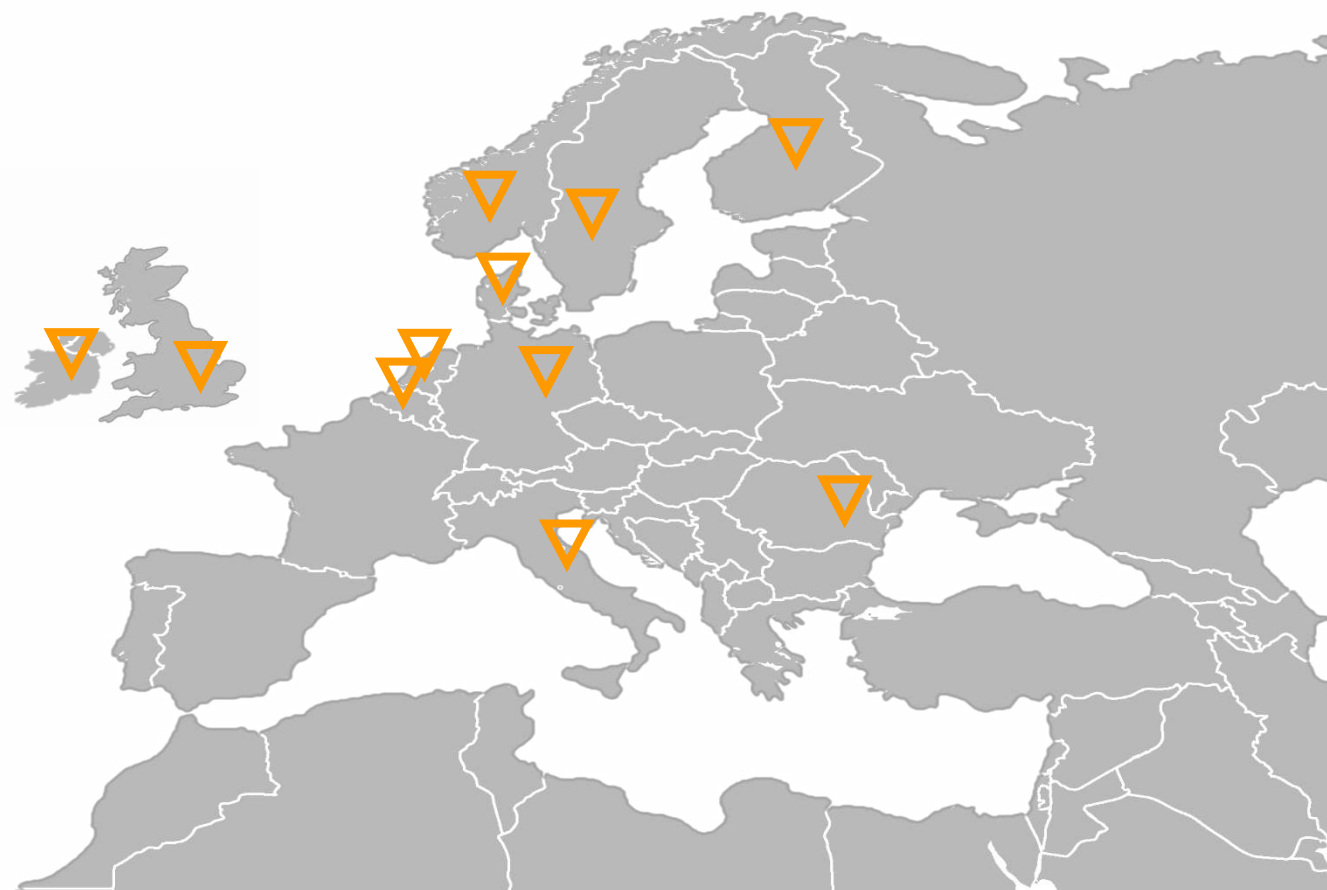
TIBER-IT

TIBER-SE

TIBER-NO

TIBER-FI

CBEST (UK)



Experiences with TIBER



Key success factors

1. White team members
2. Involve third party service providers
3. Open communication between White/Red team
4. Trust between providers and test subject
5. Scope
6. Scenario identification

Overall recommendations

1. Ensure you prepare yourself for a TIBER assessment
2. Identify Critical Business Functions
3. Basic security hygiene
4. Perform table top exercises
5. Perform purple team sessions
6. Perform a Red Team test before TIBER and remediate findings

Links to TIBER documentation

- [TIBER framework documentation](#)
-  Rob Wassink (DNB)
-  Vincent Waart (EY)