TF-CSIRT
TRANSITS

# TRANSITS I

## Legal Module

**Presenter**

Authors: Andrew Cormack, Nicole Harris and Silvio Oertli.
Version: 7.0.

# Learning Objectives

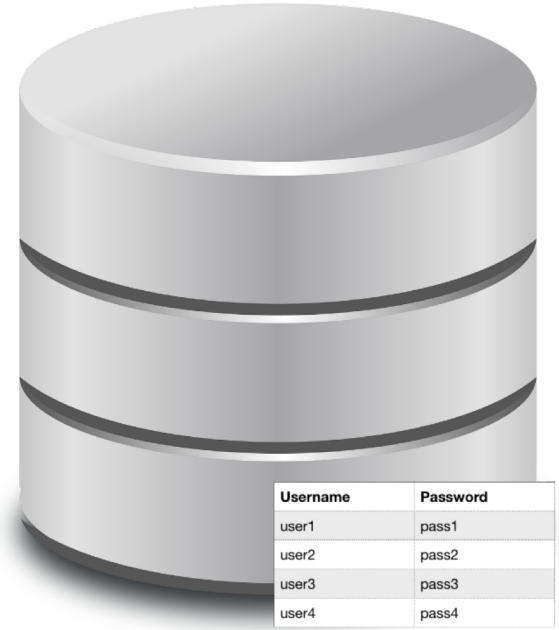
# Session Plan

- Introduction
- Which Issues arise when it comes to …
    1. CSIRTs and the Law
    2. Logging
    3. Looking at Content
    4. Scanning for Vulnerabilities
    5. Takedown Requests
    6. Working with Law Enforcement
    7. Working with Others
    8. Managing Vulnerabilities
- Homework

TF-CSIRT
TRANSITS

# Part One: Introduction

# Discussion 1: CSIRTs and the Law



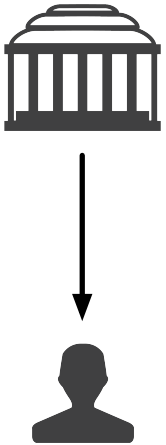

- You receive a Dump with Username / Password.
- It has been used to access a Site in the “Dark Web”.
- Users are from your Organisation and others.
- Police ask for a copy.

- What can / should / must you do?
- … your CSIRT?
- … your Organisation?

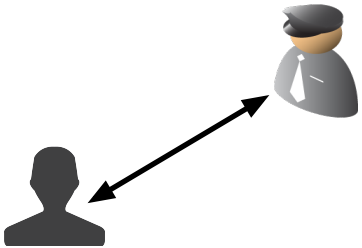
## Learnings

- Legal issues are going to arise, whether you like or not!
- Old laws, new laws and ICT Laws.
- Different sets of law:
  - Public -> limiting societally bad things such as drugs, firearms, hacking.
  - Private -> on how one party can be required to repair damage it has caused to another.
  - Cooperation -> requiring / allowing you to help state entities such as police.

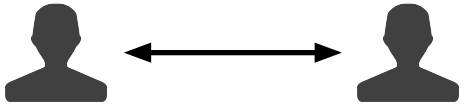
# Public & private Law



Public Law

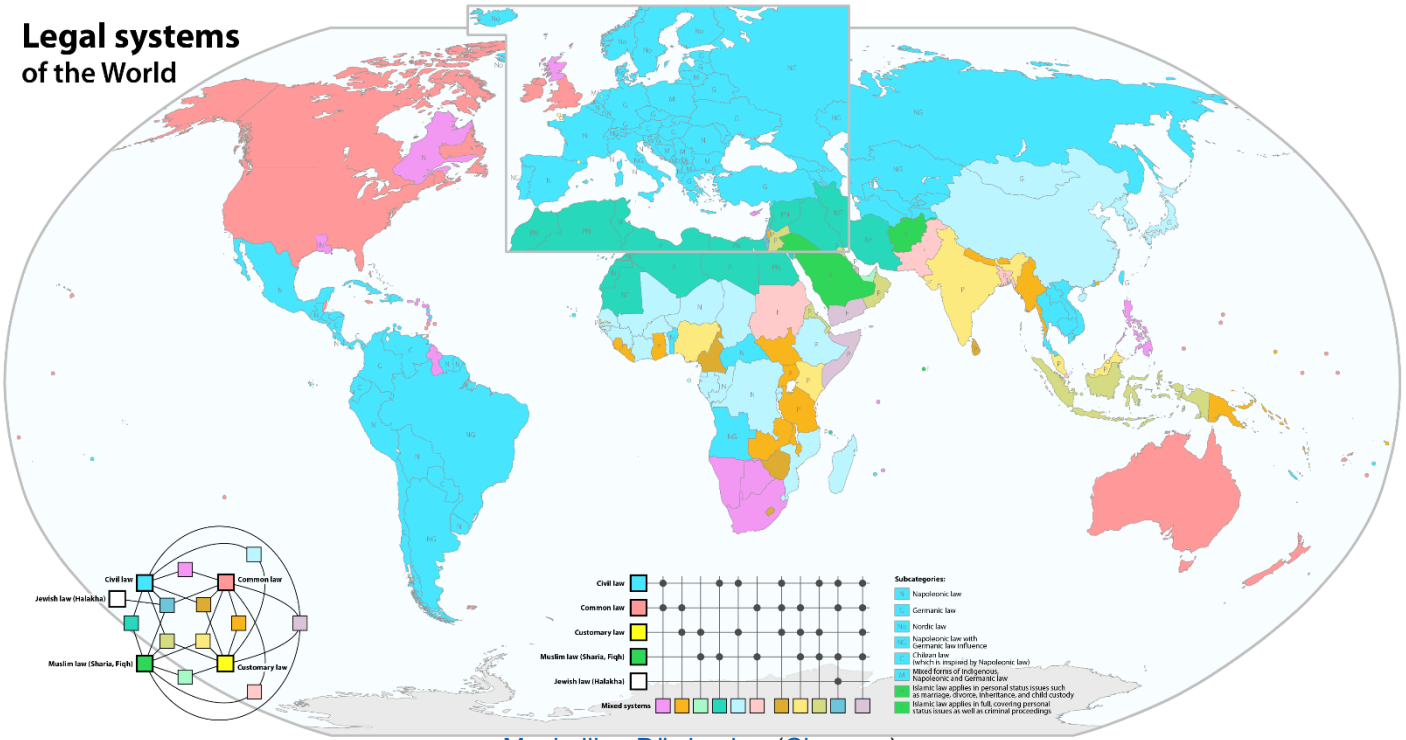


Cooperation



Private Law

# Law differ between countries




Maximilian Dörrbecker (Chumwa)

TF-CSIRT
TRANSITS

# Part Two: Scenarios

# Discussion 2: Logging


- “Bad guys” have obtained username / password for some of your webmail users.
- They are using credentials to send phishing e-mails to other local users.
- You like to find out who’s compromised.

- What logs do you need for investigation?
- What legal issues arise?

# Logging

## Learnings

- Logs contain personal data
- Only use logs you need for this investigation
- Process tell you which logs you need
- How long to keep them?

## Variability

- EU + some states -> general personal data law (based on GDPR / Convention 108)
- US + some states -> based on sector-specific law
  - Health
  - Teaching
  - Video rentals
  - Financial

# General Data Protection Act (GDPR)

European law (since 2018); influential elsewhere too.

Applies to all processing of personal data (including email/IP/MAC addresses).

Explicitly encourages incident response:

- Implicitly requires it, via breach notification.

Legitimate interest tests:

- Process minimum data required to achieve purpose.
- Ensure benefit of processing justifies risk to individuals.

Key point: Incident Response improves protection of users' personal data & privacy!

# Discussion 3: Looking at Content

- A chip vendor for Mobilephones implements FotA Updater.
- The routine sends personal data to chip vendor's IP.
- Data transfer is unencrypted.
- You intercept traffic to specific IP Addresses (to determine scenario and users affected).

- What might you consider?
- What legal issues arise?

## Looking at Content

TF-CSIRT TRANSITS

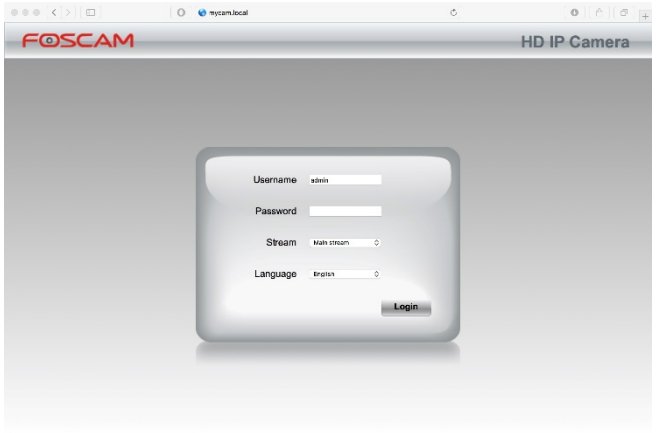
### Learnings

- Access to content more protected than access to metadata
- Inspect content only for specific investigations
- Need to implement safeguards
- Specific legislation on telecommunication
- European Convention on Human Rights (Art. 8)
  - Right to respect for private and family life, home and correspondence

### Variability

- High as well between countries as between types of network
- Private / corporate vs. public / telecommunication

# Discussion 4: Scanning for Vulnerabilities




- A new DDoS amplification is discovered.
- You as CSIRT like to determine vulnerable devices / services.
- There is a login screen at Port 80.
- You try to access with default password libraries.

- Are your actions legal?

# Scanning for Vulnerabilities

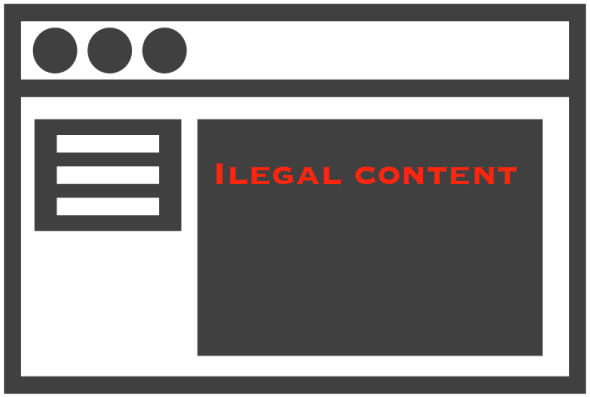
## Learnings

- A lot of countries have “unauthorized access” laws
- It might depend on Purpose / Protected / Authorised / Harm

## Variability

- High
- Law often unclear even within countries

# Discussion 5: Takedown Request




- You receive a complaint about illegal Material on a website
- The website belongs to your constituency
- You've been asked to remove the content and prevent it from being republished

- What do you do?
- What material is illegal in your country?

# Takedown Request

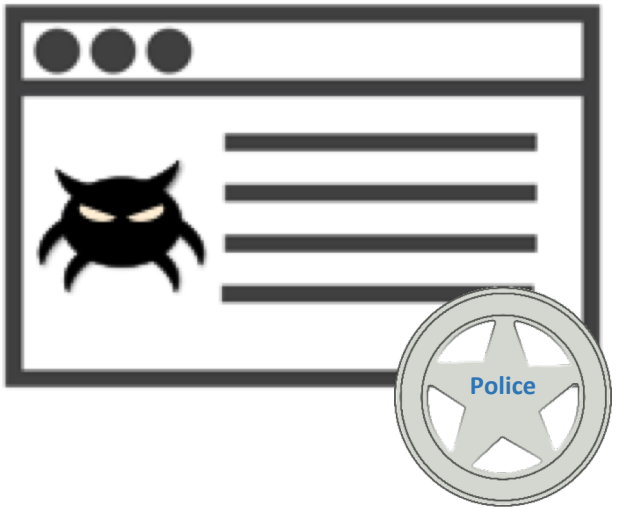
## Learnings

- Different types are covered by different laws
  - Copyright, Software licensing. Terrorism. Hate speech. Cryptominers. Malware
- Requirements to prevent re-publication are rare but not unknown
- There may be types of material that you are required to report if discovered
- It might be that you are on the other side and like to take down from somewhere else

## Variability

- High
- Depends on
  - Country
  - Type of material
  - Type of service

# Discussion 6: Working with Law Enforcement




- Your Organisation runs its infrastructure in the cloud
- A Server is compromised and distributes malware
- The police ask for logs, billing information
- The police ask for the malware

- Are you allowed to give away the data?
- What changes if the police is foreign?

# Working with Law Enforcement

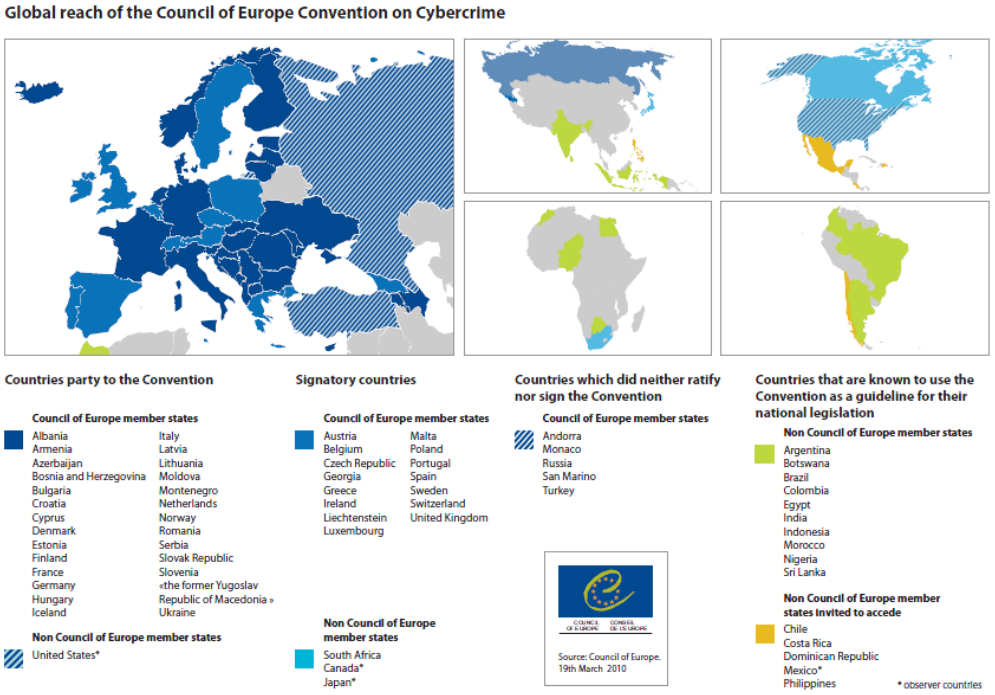
## Learnings

- National law may require / allow / prohibit disclosure to law enforcement
- International disclosure may additionally require you to think about
  - Mutual Legal Assistance
  - Cybercrime Convention
  - Bilateral treaties
  - US Cloud ACT
  - EU E-Evidence proposal
- Talk with the Police and your local lawyer

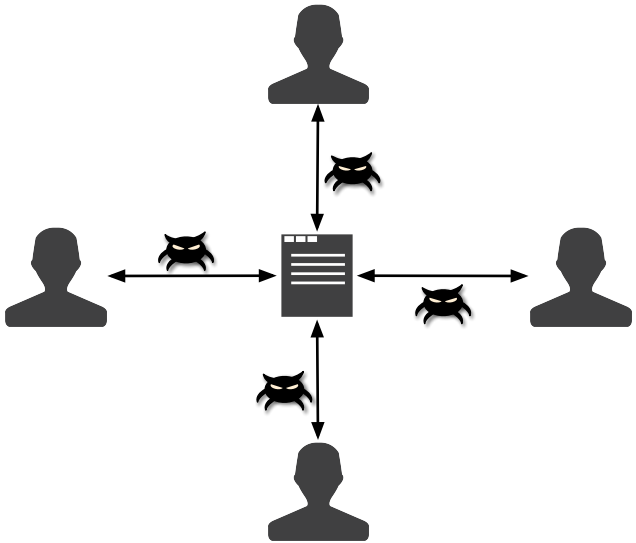
## Variability

- Very High
- Based on
  - Countries
  - Types of investigations
  - Types of content

# Cyber Crime Convention (Budapest Convention)



# Discussion 7: Working with Others



- You analyzed a new piece of malware
- The malware was distributed through E-Mail
- You would like to share:
  - Pattern / Indicators of Compromise with other CSIRTs
  - Malware and infected E-Mails through MISP

- What could be the problem with sharing?
- How could you avoid this?

TF-CSIRT TRANSITS

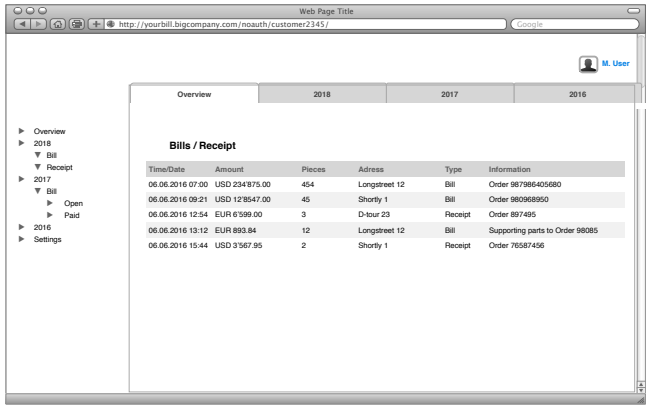
## Learnings

- Risk of sharing must be justified by benefits
- Reduce risks by safeguards such as Traffic Light Protocol (TLP)
- Sharing Malware may raise ”Hacking tools” issues

## Variability

- Data protection / privacy issues relatively standard
- ”Hacking tools” understanding might vary

# Discussion 8: Managing Vulnerabilities




- Two weeks ago someone report a vulnerability in your web application
- He used the main E-Mail Address of the organization
- He accessed details of customers by careful choice of URL
- Evidence was a screenshot
- E-Mail routed to corporate lawyers, who threatening to report to the police

- What legal issues arise?
- How could they been avoided?

## Learnings

- Researcher appears to have been trying to help the organization
- Legal Department's response treats him as enemy
- Better to have published vulnerability report policy
- Liability might arise to individuals whose data are put at risk by the unfixed vulnerability
- Advanced issues including laws against reverse engineering of software

## Variability

- Much of the work in Coordinated Vulnerability Disclosure done by organisations in the Netherlands
- Same approach should be applicable elsewhere

TF-CSIRT
TRANSITS

# Part Three: Homework

# Where to start at home

- **Find out who is your legal adviser or who is in charge to support you**
- **Find out *and record* the law for your CSIRT, e.g.**
  - Privacy / Data Protection & Monitoring
  - Scanning / Pentesting
  - Notice and Takedown
  - Rules for working with law enforcement
  - Information Sharing
  - Vulnerability Management / Vulnerability Disclosure Policy

# Where to start at home

- Prepare to recognise and handle legal notices
- Make sure policies & procedures support working lawfully

TF-CSIRT
TRANSITS

# Thank you
# Any Questions?

Authors: Andrew Cormack, Nicole Harris and Silvio Oertli.
Version: 7.0.