TF-CSIRT
TRANSITS

TRANSITS I

Legal Module

Presenter

Authors: Andrew Cormack, Nicole Harris, Silvio Oertli and Casper Dreef.
Version: 7.2.

Let's start with a question

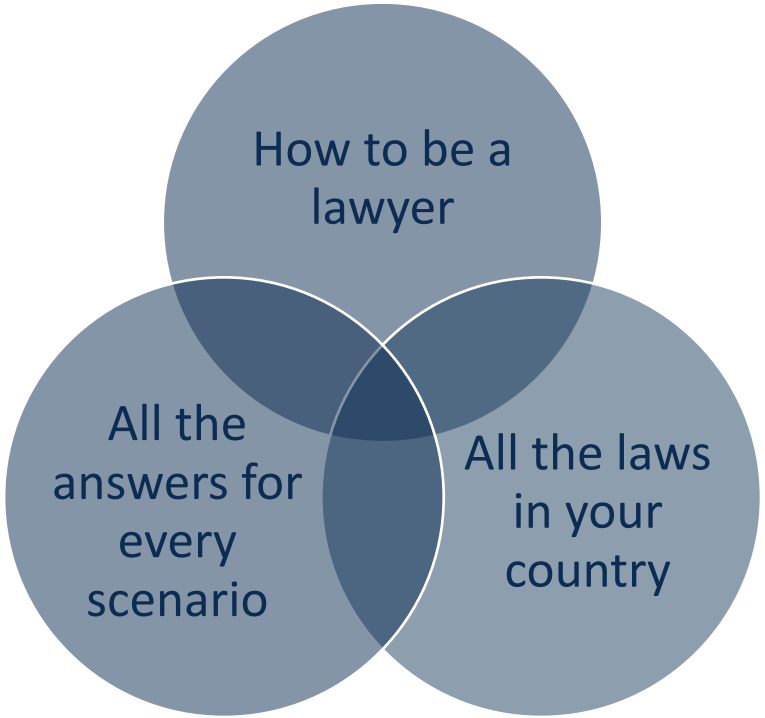
TF-CSIRT TRANSITS

What does this sign mean?

And what about this sign?

Learning Objectives

What Won't We Learn?



Session Plan

TF-CSIRT
TRANSITS

Part One: Introduction

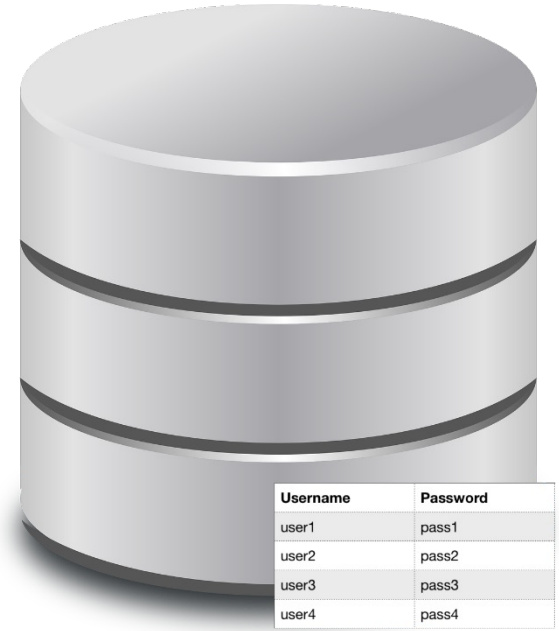
Group Discussion

What do we consider to be a “cyber” crime?

Which are crimes are cyber-dependent?

Which are crimes can be cyber-enabled?

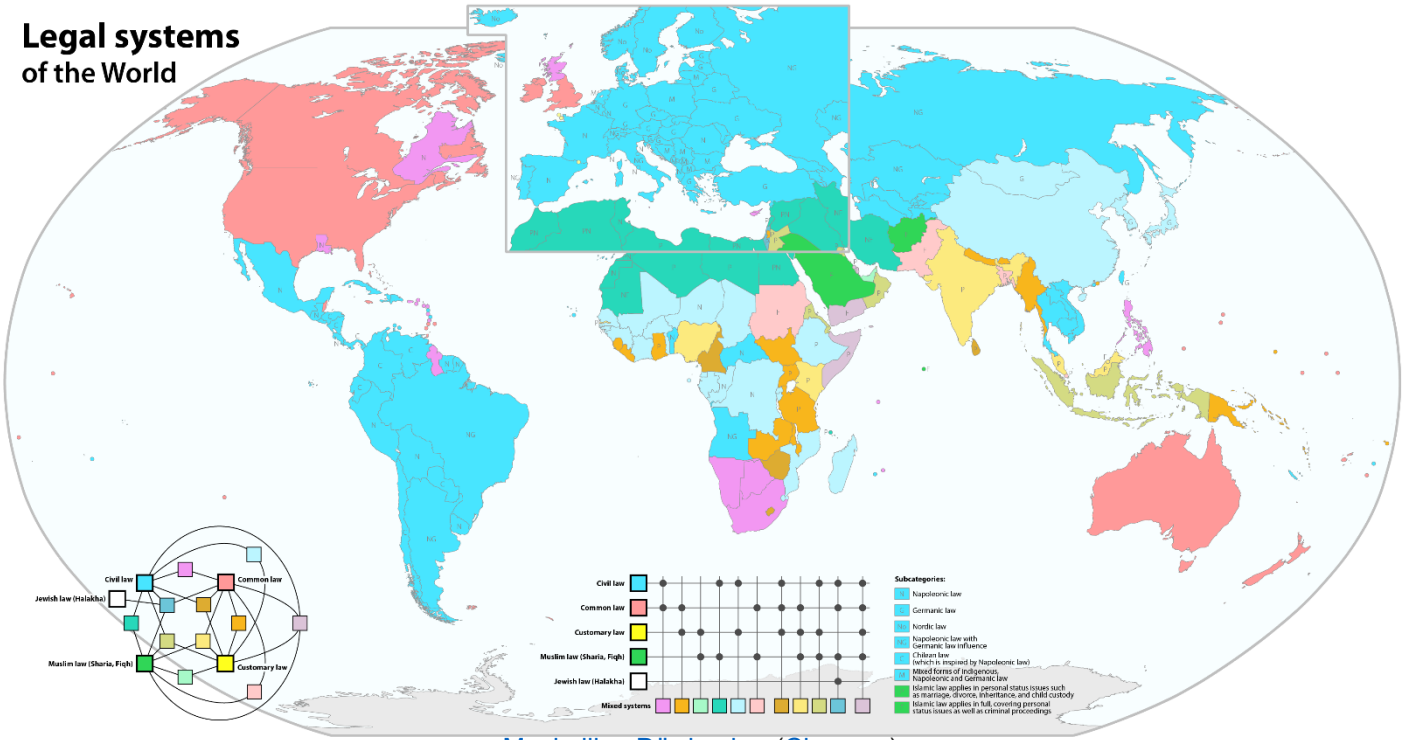
Discussion 1: CSIRTs and the Law



- You receive a dump that includes Usernames / Passwords.
- These users have accessed a site in the “Dark Web”.
- Users are from your Organisation and others.
- Police ask for a copy of the data.

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

Law differ between countries



Maximilian Dörrbecker (Chumwa)

What Do They All Mean?

Civil Law

- A codified system: law is defined by statutes (e.g. Napoleonic code).

Common Law

- Laws are based on the decision of judges following the review of cases.

Customary Law

- A general practice accepted as law.

Religious law

- a religious system or document being used as a legal source.

Strategy

EU Cyber Security Strategy for Digital Decade

European Declaration on Digital Rights and Principles

Use / Misuse

High common level of cybersecurity

NIS2 Directive (EU) 2022/2555

Cyber Solidarity Act 2023/0109

Improve response to cyber threats

EUCC

ENISA

CSIRTs Network

Resilience of products and services

Cyber Resilience Act 2022/0272

Critical Entities Resilience Directive (CER)

EU Cyber Security Regulation (EU) 2019/881

Cyber policy (ENISA), certification and collaboration

Joint Cyber Unit - ENISA, CERT-EU, EC3

Crime

Child Abuse Regulation (EU) 2021/1232

Anti-fraud Directive (EU) 2017/1371

Budapest Convention (CETS) 185

Rights

European Convention on Human Rights

European Patent Convention

IPR Directive 2004/48/EC

ePrivacy Directive 2002/58/EC

GDPR (EU) 2016/679

Learnings

- Legal issues are going to arise, whether you like or not!
- Old laws, new laws and ICT Laws.
- Laws and legal systems are different country to country – know the topics you should be aware of.

TF-CSIRT
TRANSITS

Part Two: Scenarios

Discussion 2: Logging

- “Bad guys” have obtained usernames / passwords for some of your webmail users.
- They are using credentials to send phishing e-mails to other local users.
- You would like to find out who is 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)

TF-CSIRT
TRANSITS

European law (since 2018); influential worldwide

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

Explicitly encourages incident response:

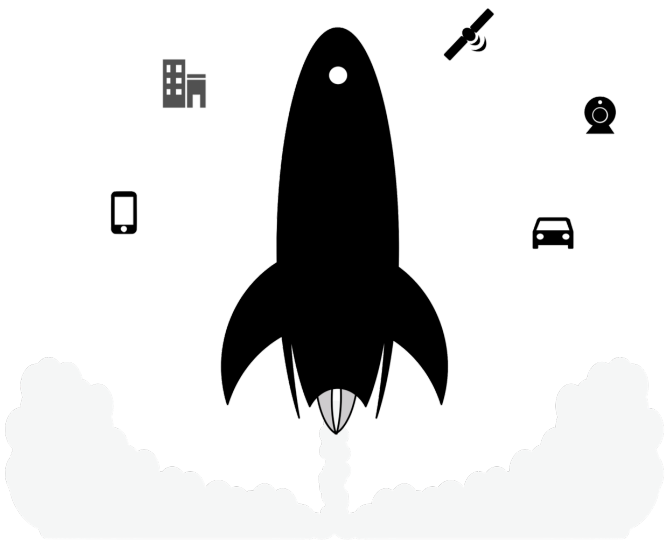
- Implicitly requires it, via breach notification

Legitimate interest tests:

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

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

Discussion 3: Looking at Content



- A chip vendor for Mobilephones implements a FotA Updater.
- The routine sends personal data to the 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

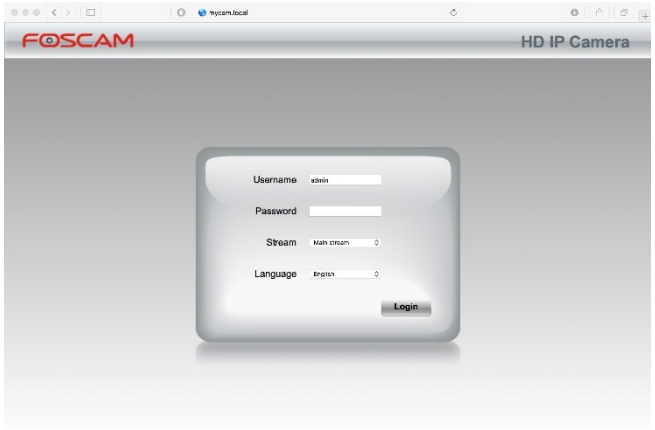
Learnings

- 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 has been discovered.
- You as a CSIRT would 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 hosted 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

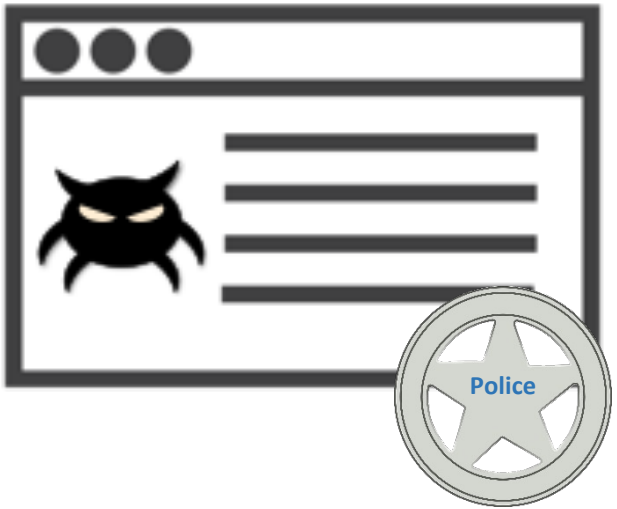
Learnings

- 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

TF-CSIRT TRANSITS

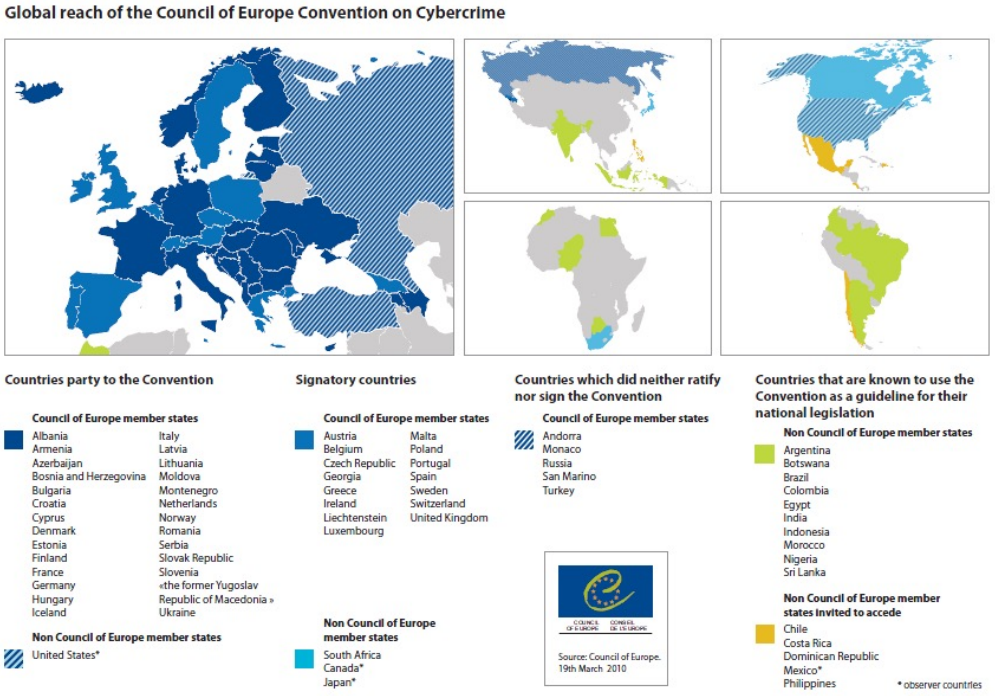
Learnings

- 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

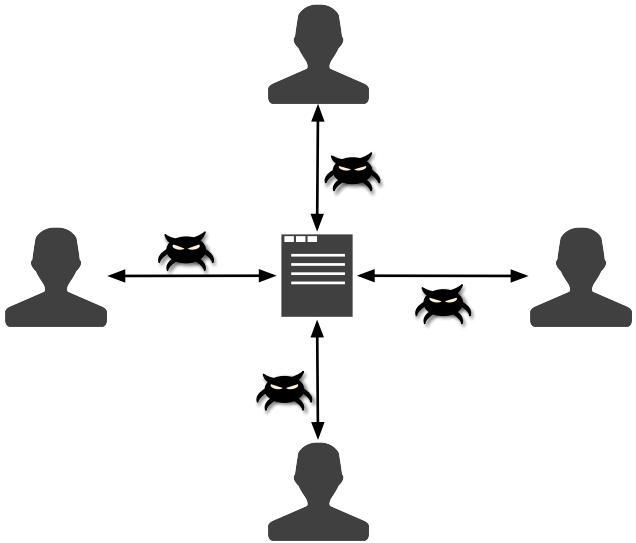
Variability

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

Cyber Crime Convention (Budapest Convention)



Discussion 7: Working with Others



- You analysed 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?
- What obligations might you have to share?

What is the NIS-2 directive about?

NIS2: Essential or Important?

TF-CSIRT TRANSITS

SECTORS OF HIGH CRITICALITY (Annex I)

- Energy
- Transport
- Banking
- Financial Market Infrastructure
- Health
- Drinking water
- Waste Water
- Digital infrastructure
- ICT Service management
- Public Administration
- Space

OTHER CRITICAL SECTORS (Annex II)

- Postal and courier services
- Waste management
- Chemical industry and supply chain
- Food supply chain
- Manufacturing (limited)
- Digital providers
  - Online marketplace
  - Search engines
  - Social networking services platforms
- Research organisations

TF-CSIRT TRANSITS

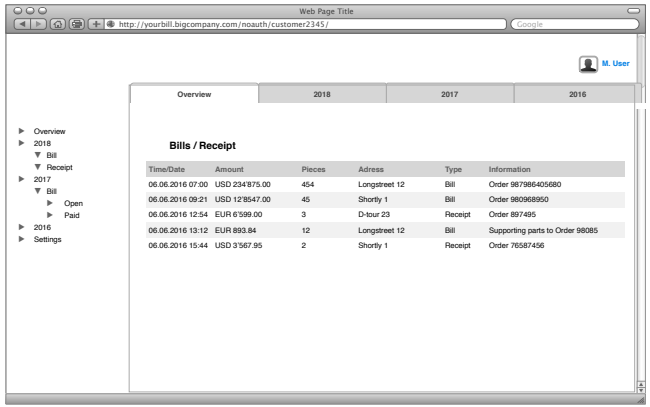
Learnings

- 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 reported a vulnerability in your web application
- They used the main e-mail address of the organisation
- They accessed details of customers by careful choice of URL
- Evidence was a screenshot
- e-mail was routed to corporate lawyers, who threatening to report to the police

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

Responsible Disclosure Example

GÉANT Responsible Disclosure Policy

At GÉANT, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present. If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

What do we expect from you?

Ensure that you do not cause any damage while the detected vulnerability is being investigated. Your investigation must not in any event lead to an interruption of services or lead to any details being made public of either the asset manager or its clients.

Please do the following:

- Send your findings to cert@oc.geant.net:
- Encrypt your findings using our PGP KEY: GEANT CERT - PGP Key ID: 0x99833085 / Fingerprint: 3CBF F211 8305 635D 5839 BB27 BA6B F34A 9983 3085
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

Also consider:
RFC9116: https://securitytxt.org/
BCP21 / RFC2350: https://www.rfceditor.org/rfc/pdfrfc/rfc2350.txt.pdf

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

TF-CSIRT TRANSITS

1

Find out who is your legal adviser or who is in charge to support you

2

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

3

Prepare to recognise and handle legal notices

4

Make sure policies & procedures support working lawfully

TF-CSIRT
TRANSITS

Thank you
Any Questions?

Authors: Andrew Cormack, Nicole Harris, Silvio Oertli and Casper Dreef.
Version: 7.2.