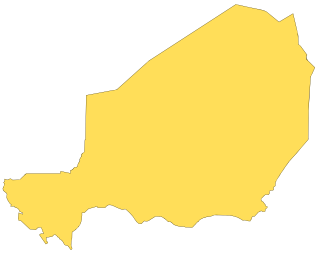
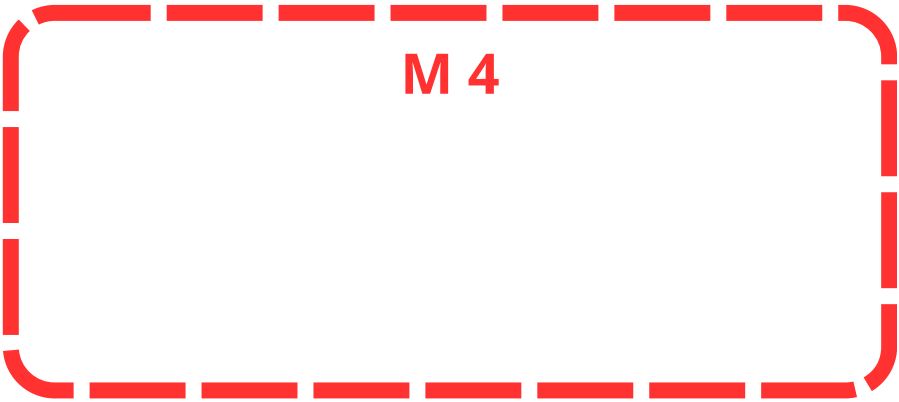
M 4

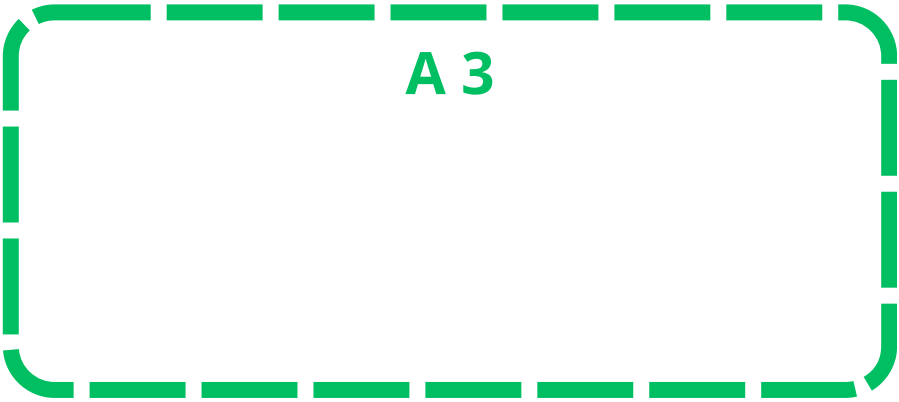


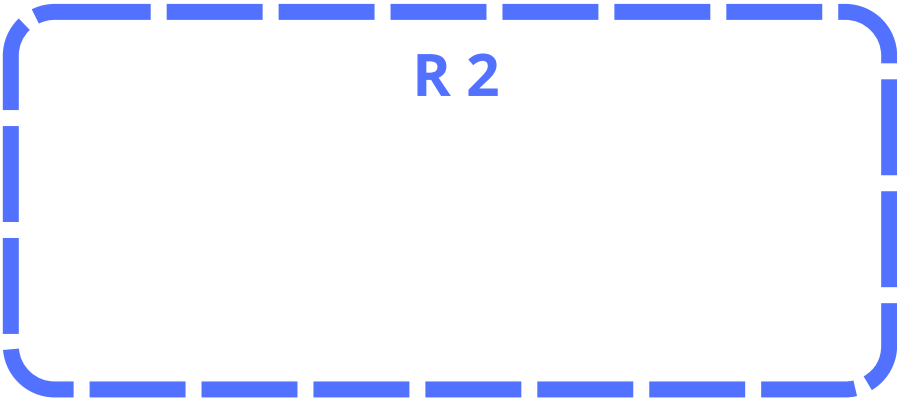
Aujourd'hui, c'est la fin de nos 3 mois passés au Niger en voyage humanitaire. A l'auberge de jeunesse de Niamey où nous passons la nuit, je décide de récupérer mon appareil photo Reflex - Nikon D3000 - Noir + Objectif Nikon AF-S DX 18-55 mm f/3.5-5.6 G VR et ma clé USB Lexar 32 Go et me dirige vers une salle où deux ordinateurs sont mis à disposition. Je passe une petite heure à les trier et les ranger sur ma clé puis je rejoins mes collègues devenus mes amis pour le dîner. A cette occasion, Lucas nous rappelle qu'il faut que je leur envoie absolument toutes les photos que j'ai prises mais également que Pablo envoie tous les audios qu'il a pu enregistrer sur place, surtout celui de l'âne qui se promenait dans le village et qui faisait de nombreux bruits un peu bizarres dignes des toulousains à la troisième mi-temps. Je décide donc de leur montrer toutes les photos sur l'ordinateur de Matteo. Je mets la clé USB puis j'allume l'ordinateur. Au démarrage, le Packard Bell Pavilion 15" prend du temps et nous perdons patience face à sa lenteur. Une fois en marche, l'ordinateur se connecte automatiquement au wifi de l'auberge mais nous n'avons réussi à accéder à aucune donnée.

A 3

R 2


M 4


A 3


R 2

M 4

- Installation d'un logiciel malveillant sur la clé USB
- Création d'une machine zombie
- Analyse de frappe pour récupérer les identifiants-mots de passe
- Piratage du système informatique

A 3

- Installer un antivirus
- Ne pas brancher d'équipements susceptibles d'être piratés sur son ordinateur
- Règle du 3-2-1 afin de ne pas perdre ses données

R 2

- Isoler l'appareil susceptible d'être infecté
- Réaliser une analyse antivirale de tous les appareils du réseau

Menaces:

- Installation d’un virus
- Vol de données
- installation d’un logiciel malveillant
- piratage du système informatique
- création d’une machine zombie
- analyse de frappe pour récupérer les identifiants/mdp

Anticipations:

- Ne pas brancher sa clé sur un ordinateur inconnu
- Mettre régulièrement à jour son ordinateur
- installer un antivirus
- règle du 3-2-1 afin d’éviter d’utiliser la clef USB
- Ne pas brancher d’équipement susceptible d’être piraté sur son ordinateur

Remédiations:

- Évaluer l’étendue de l’intrusion
- Changer ses mots de passe
- Formater sa clé USB
- isoler l’ordinateur susceptible d’être infecté
- réaliser une analyse antivirale complète des appareils du réseau