KYBERNETICKÝ POLYGON

VG20132015103, MV CR

PŘEDMLUVA: TYPY DOS

- nízkorozpočtový DDoS
- Botnet
- DNS Distributed Reflection DoS
- slow & low DoS

BŘEZNOVÉ ÚTOKY V ČR

- zpravodajské servery
- banky (internetové stránky)
- telekomunikační operátoři
- státní správa

ÚTOKY NA KRITICKOU INFRASTRUKTURU

- útoky na íránské nukleární zařízení

- rozvody el. sítě, plynu, …

CÍLE KYPO

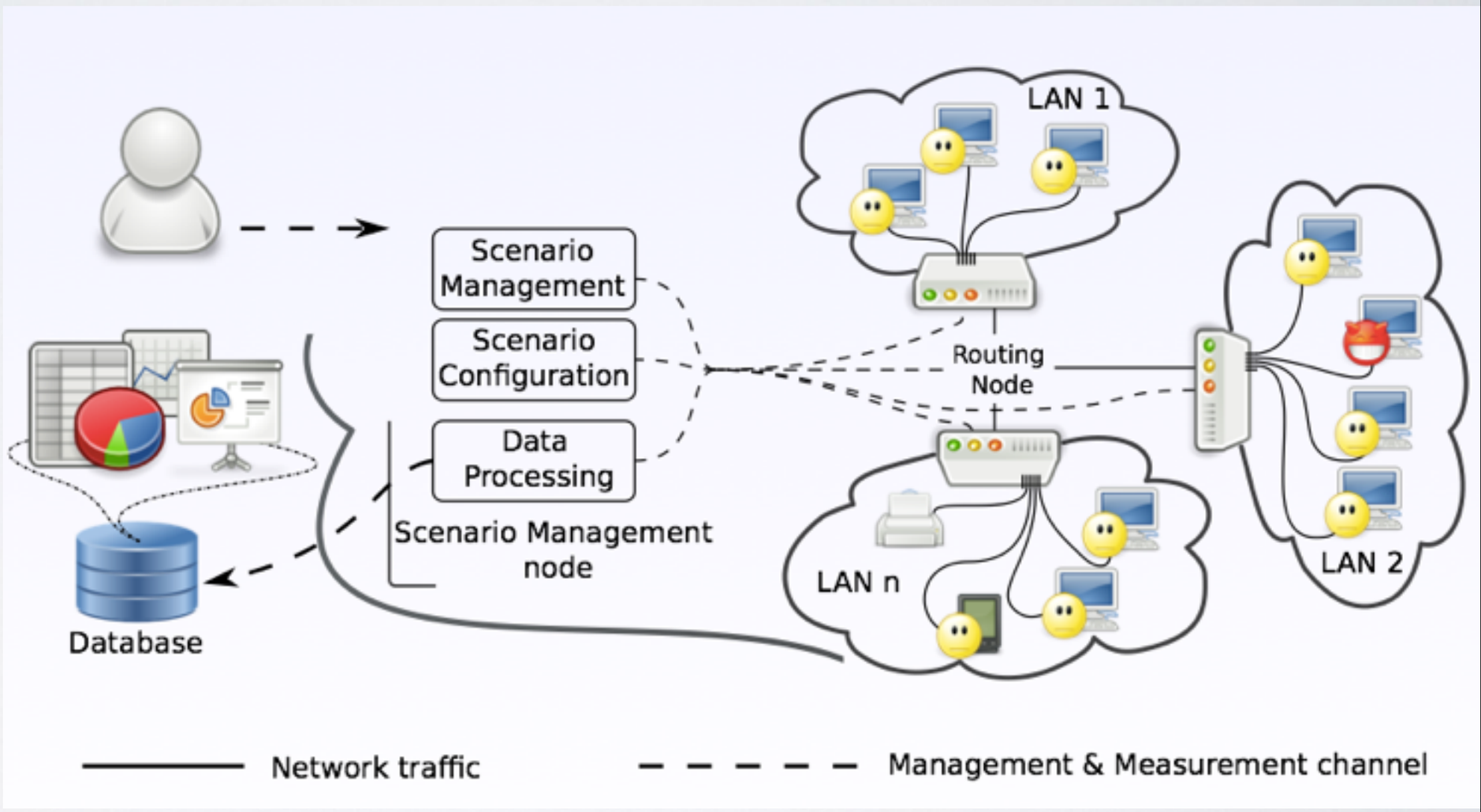
- analýza chování sítě
- analýza chování OS/aplikace
- školení
- penetrační testy
- analyzování hrozeb ohrožujících krytické infrastruktury

UŽIVATELÉ

- experti: Policie ČR, BIS (podpora konkrétního případu)
- studenti/školitelé (výuka/školení)
- kdokoliv kdo chce otestovat odolnost svého zařítení

ARCHITEKTURA

- scénáře
- cloud
- měření
- vizualizace



BEZPEČNOSTNÍ SCÉNÁŘE

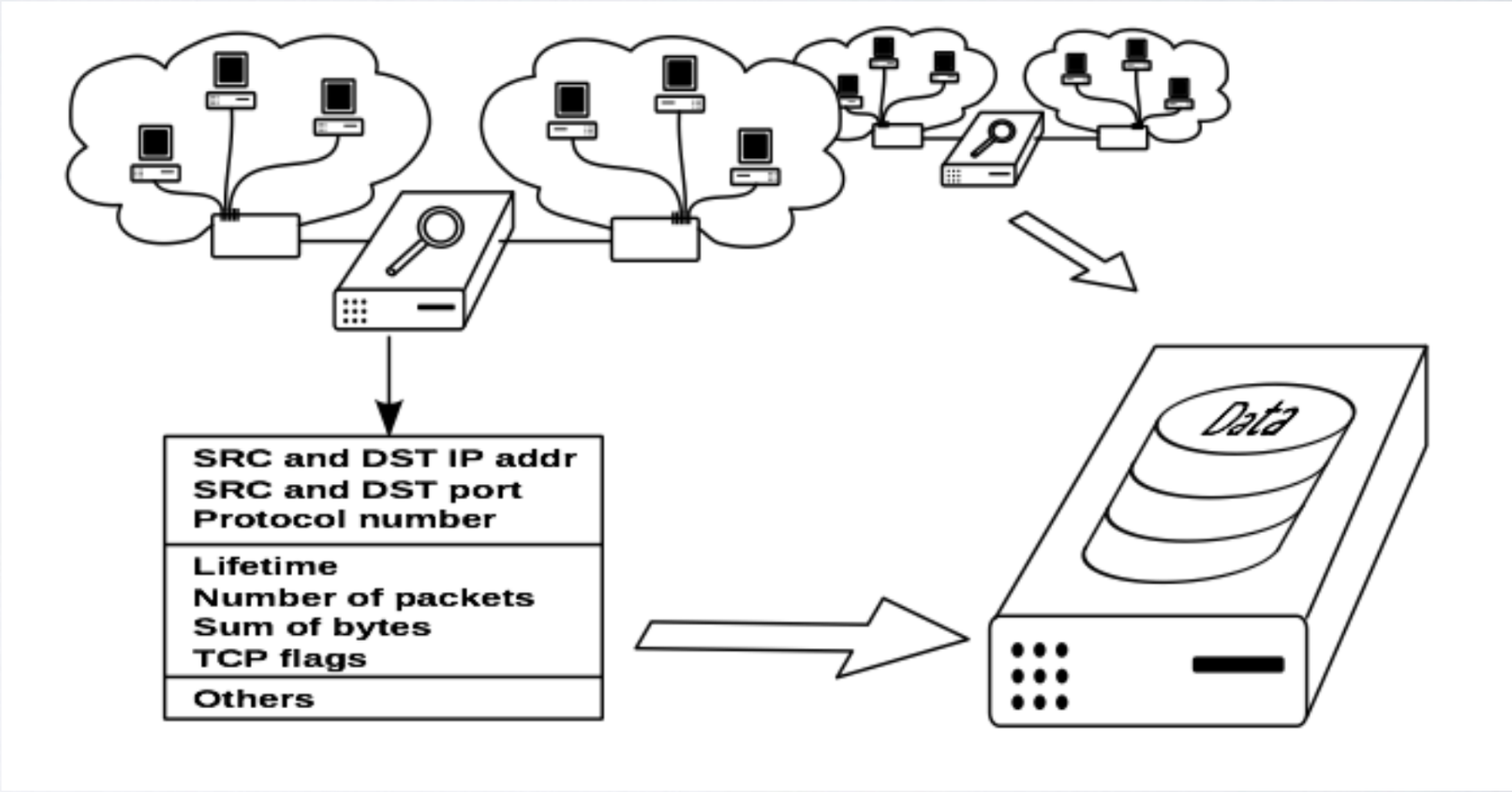
- obecně popisují průběh experimentu
  - konfigurace uzlů, síťová topologie, měřící infrastruktura, …
- založeny na principech skutečných útoků
- DDoS, šíření červů a trojských koní, expliity, phisingové útoky, kompromitace utajovaných informací,

CLOUD

- sandbox
- abstrakce nad virtualizačními frameworky
- libovolný počet virtuálních strojů
- virtuální síť (L3)
- OpenvSwitch, VLAN

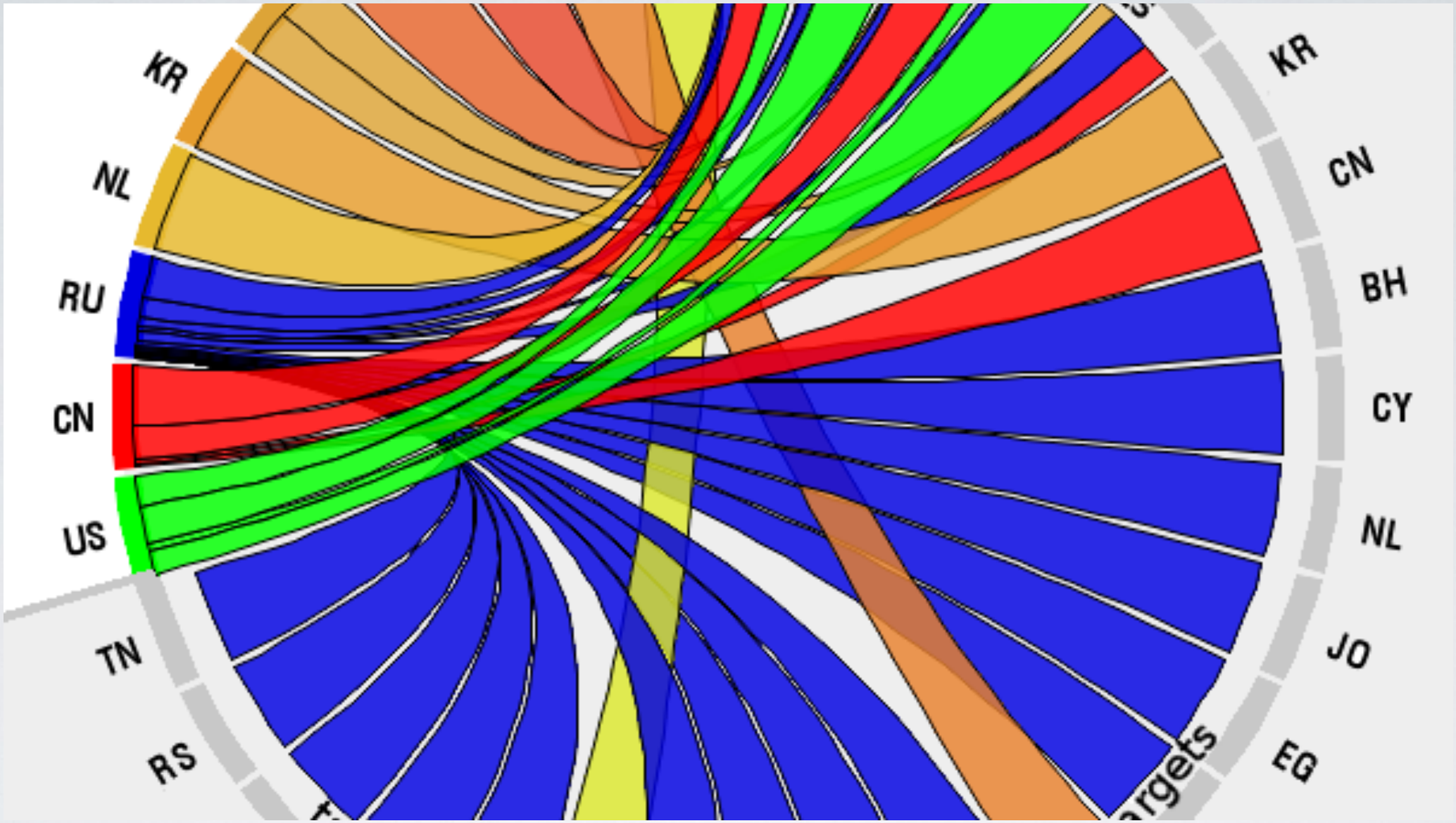
MĚŘENÍ

- sondy
- kolektor
- IPFIX
- také analýza!



VIZUALIZACE

- realtime a zpětná analýza
- pohled na důležité aspekty scénáře
- Traffic Flow
- Síťová topologie



VIZUALIZACE

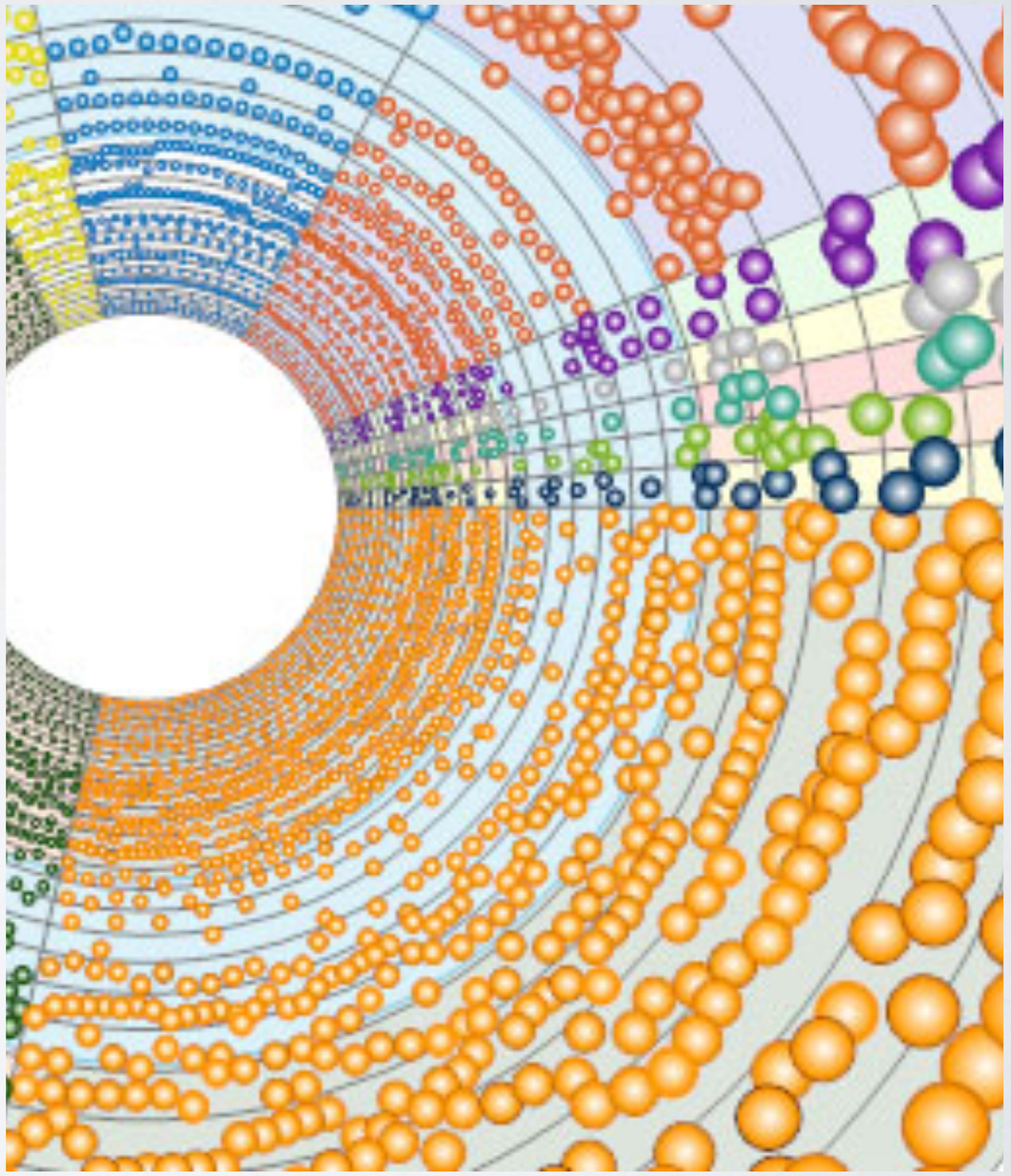
"We must see it before we can believe it"

CÍLE VIZUALIZACE

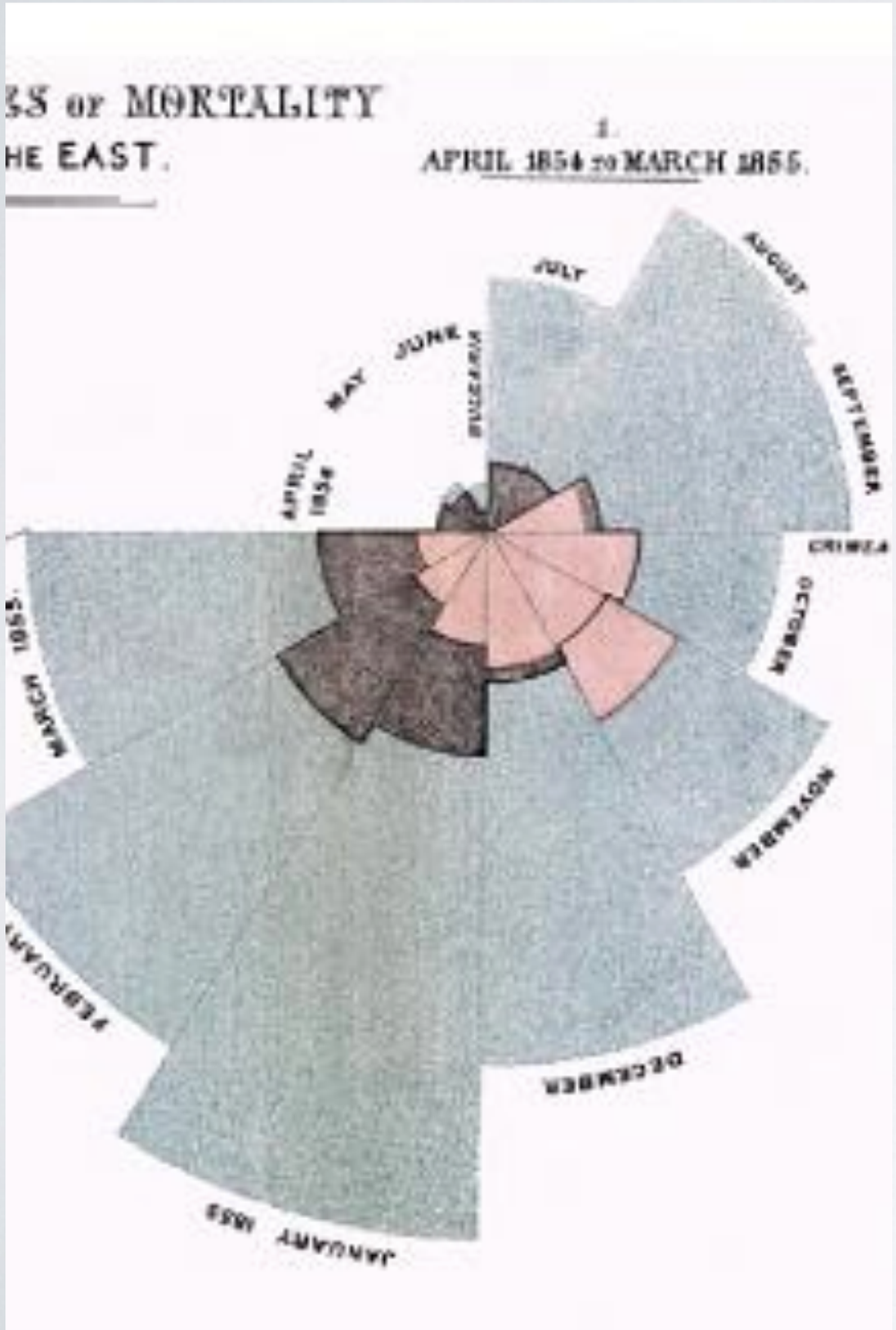
- "Seeing the unseen"
- vytvoření mentálního modelu
- explorativní analýza
- potvrzující analýza
- prezentace výsledků analýzy

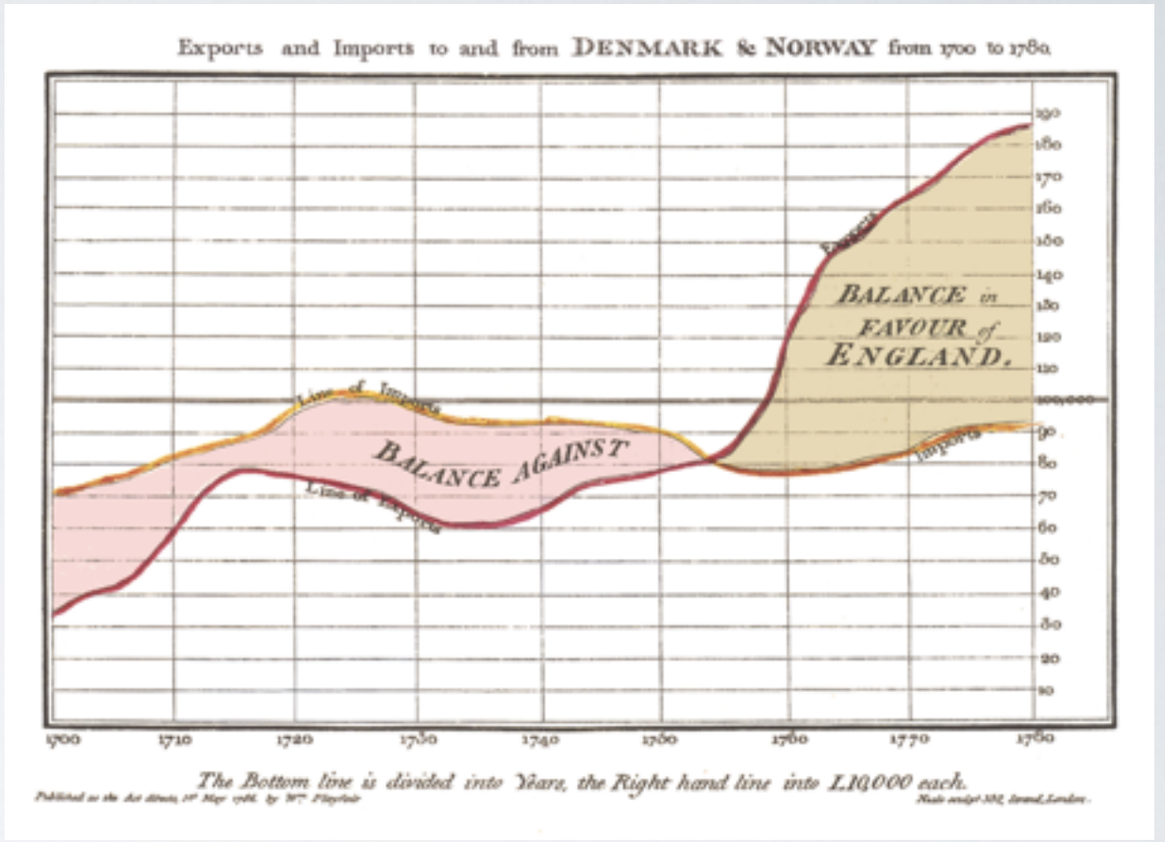
INTERAKTIVNÍ VIZUALIZACE

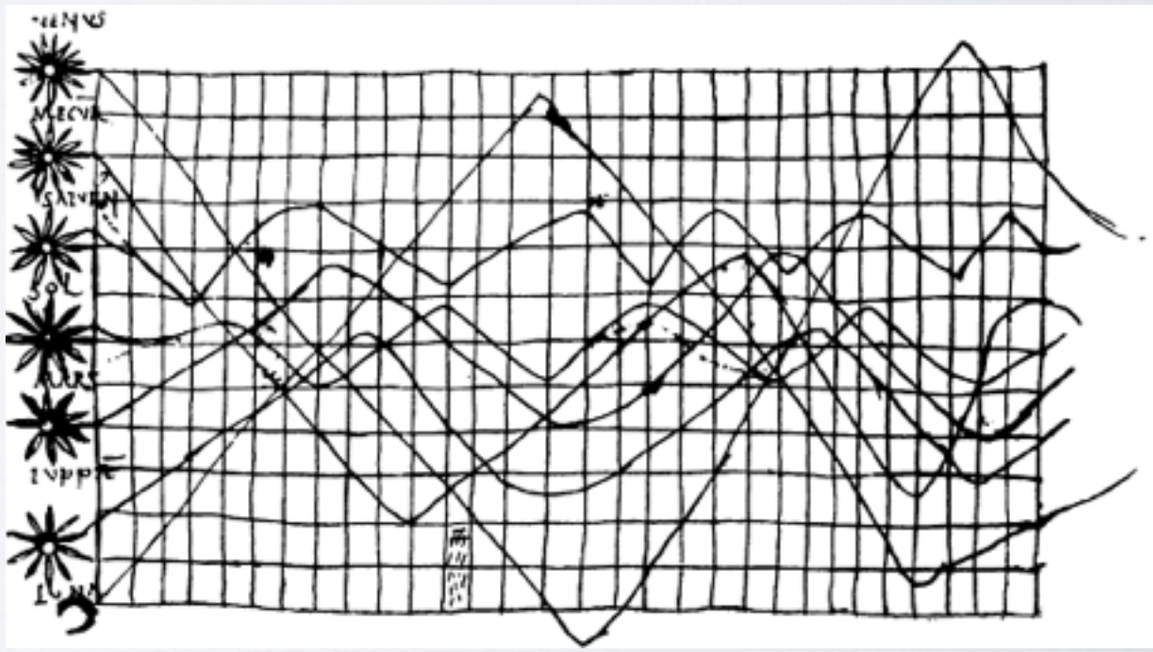
- Overview
- Zoom
- Filter
- Details-on-Demand
- Relate
- History
- Extract



JEMNÝ ÚVOD DO VZUALIZACÍ







UŽIVATEL VIDÍ CO CHCE VIDĚT

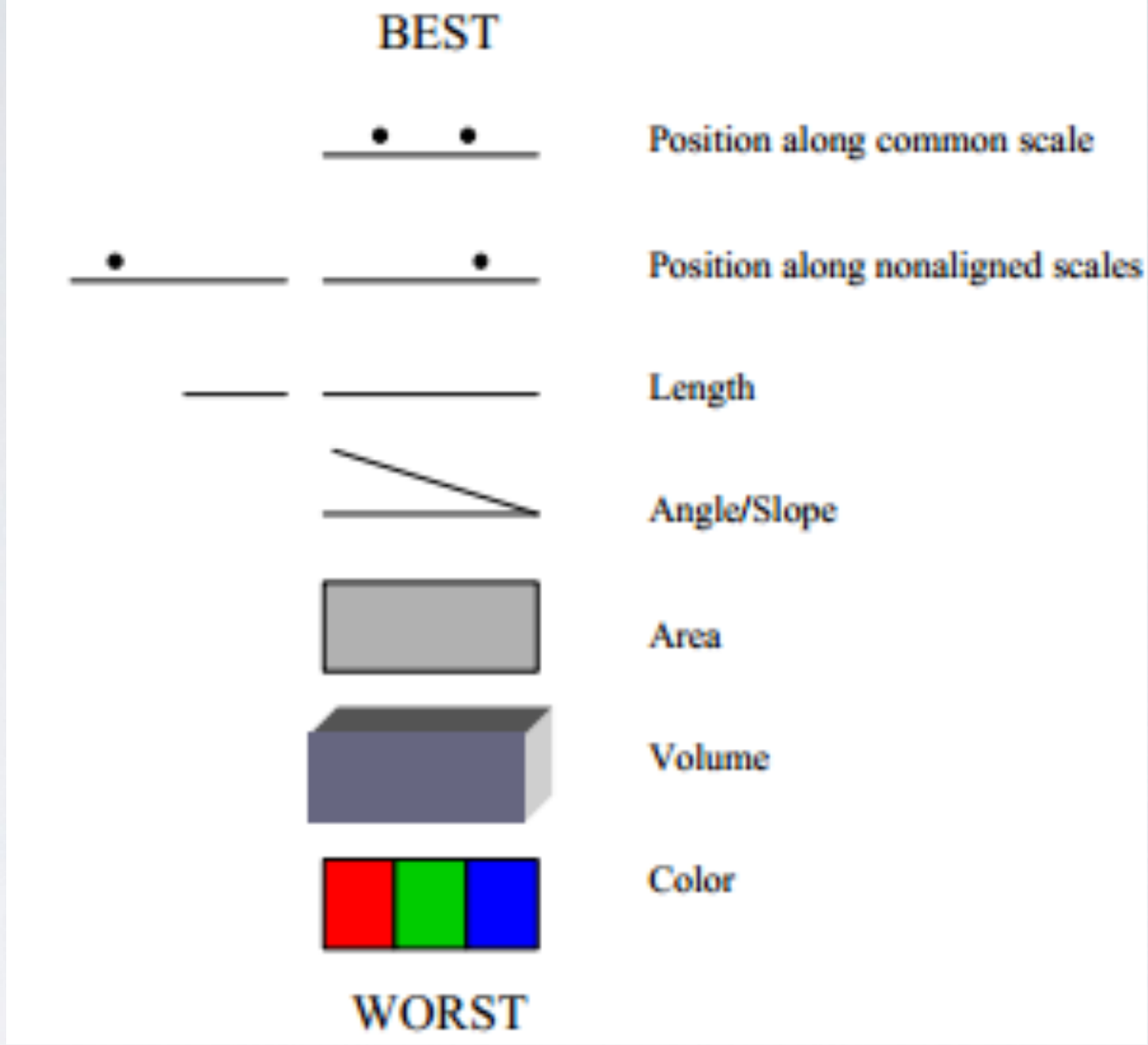
VEDENÍ

ANOMÁLIE

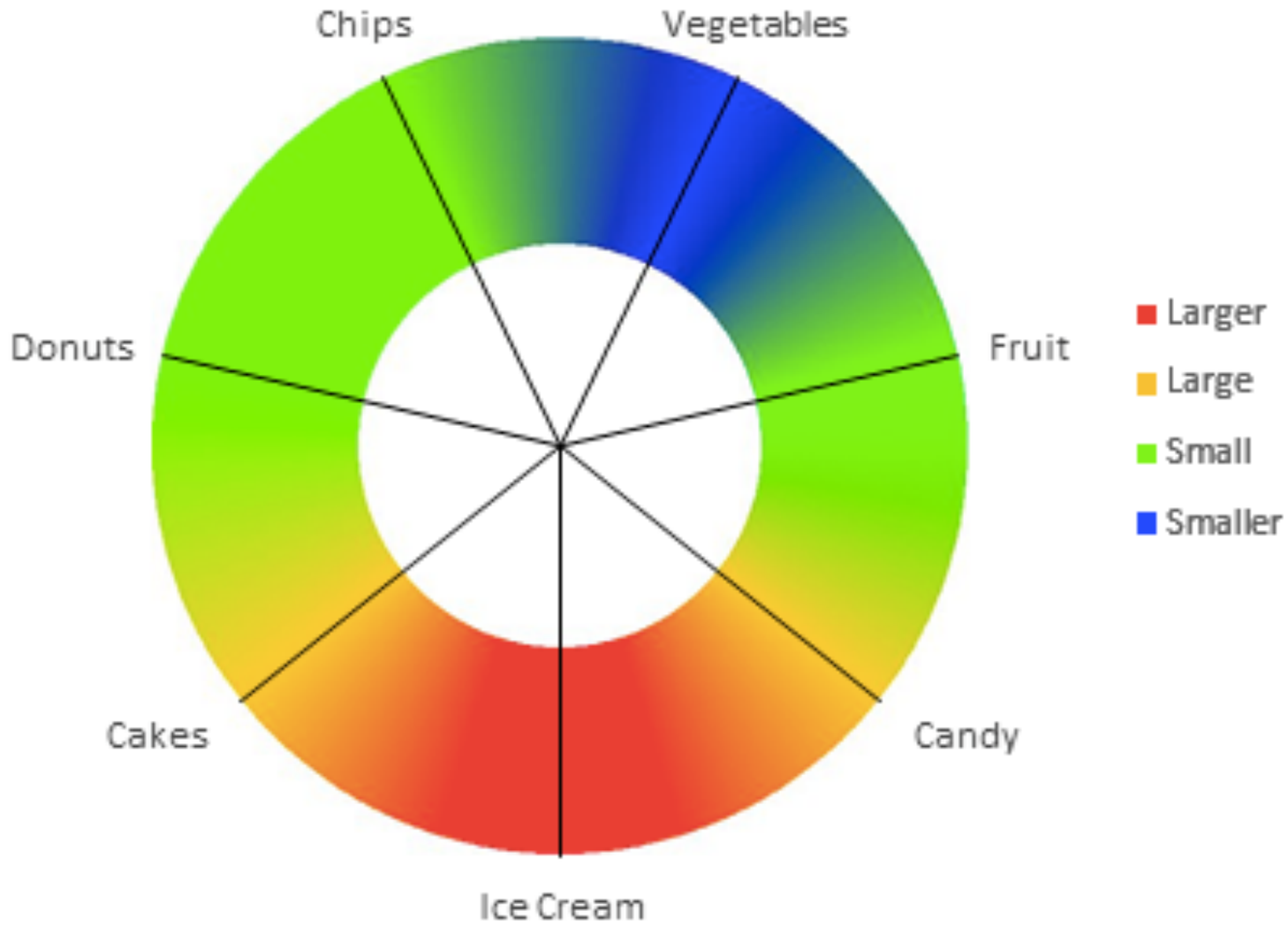
FORM FOLLOWS FUNCTION

Ornament and crime

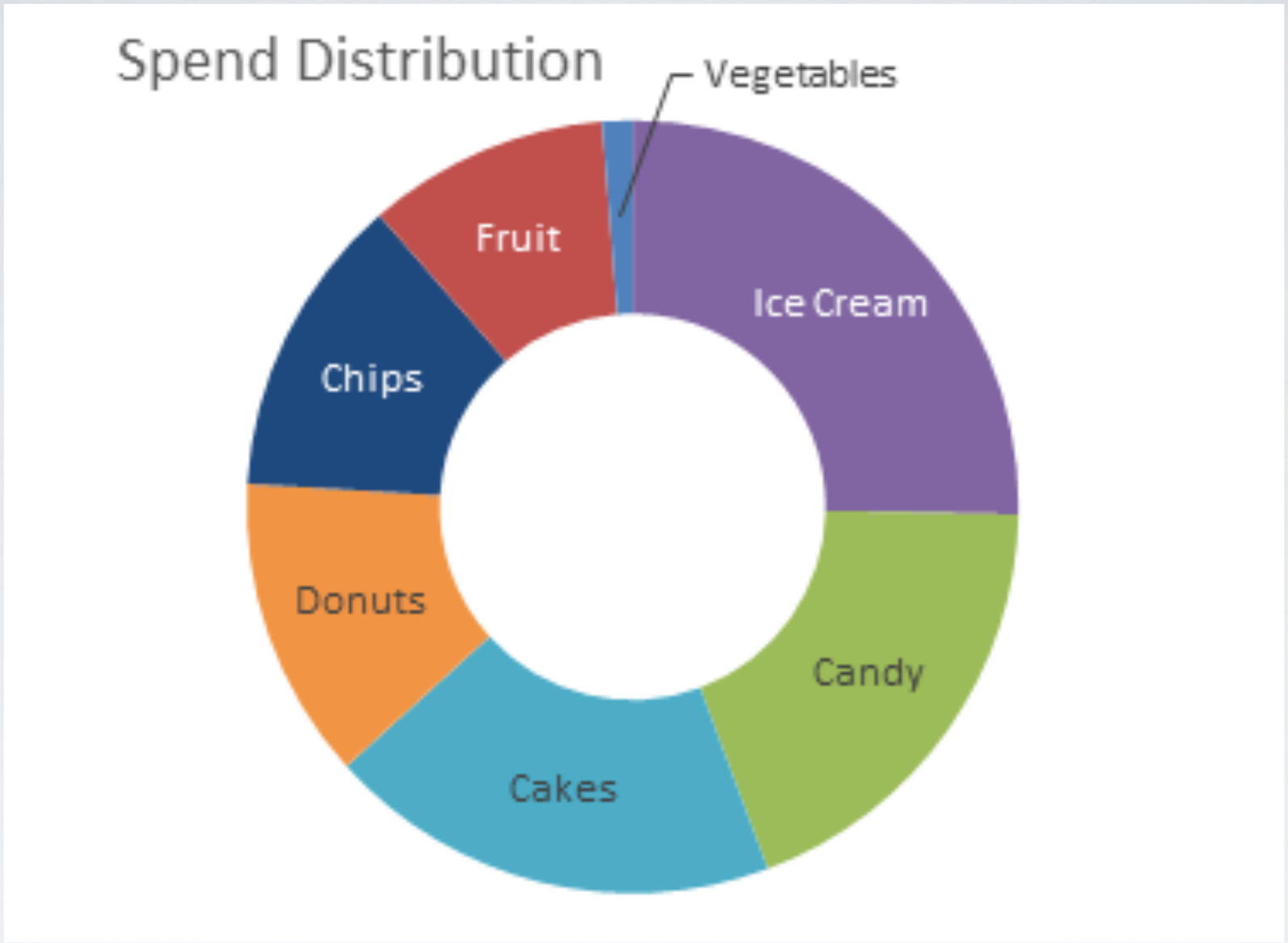
Cleveland (1994) graphical features hierarchy.



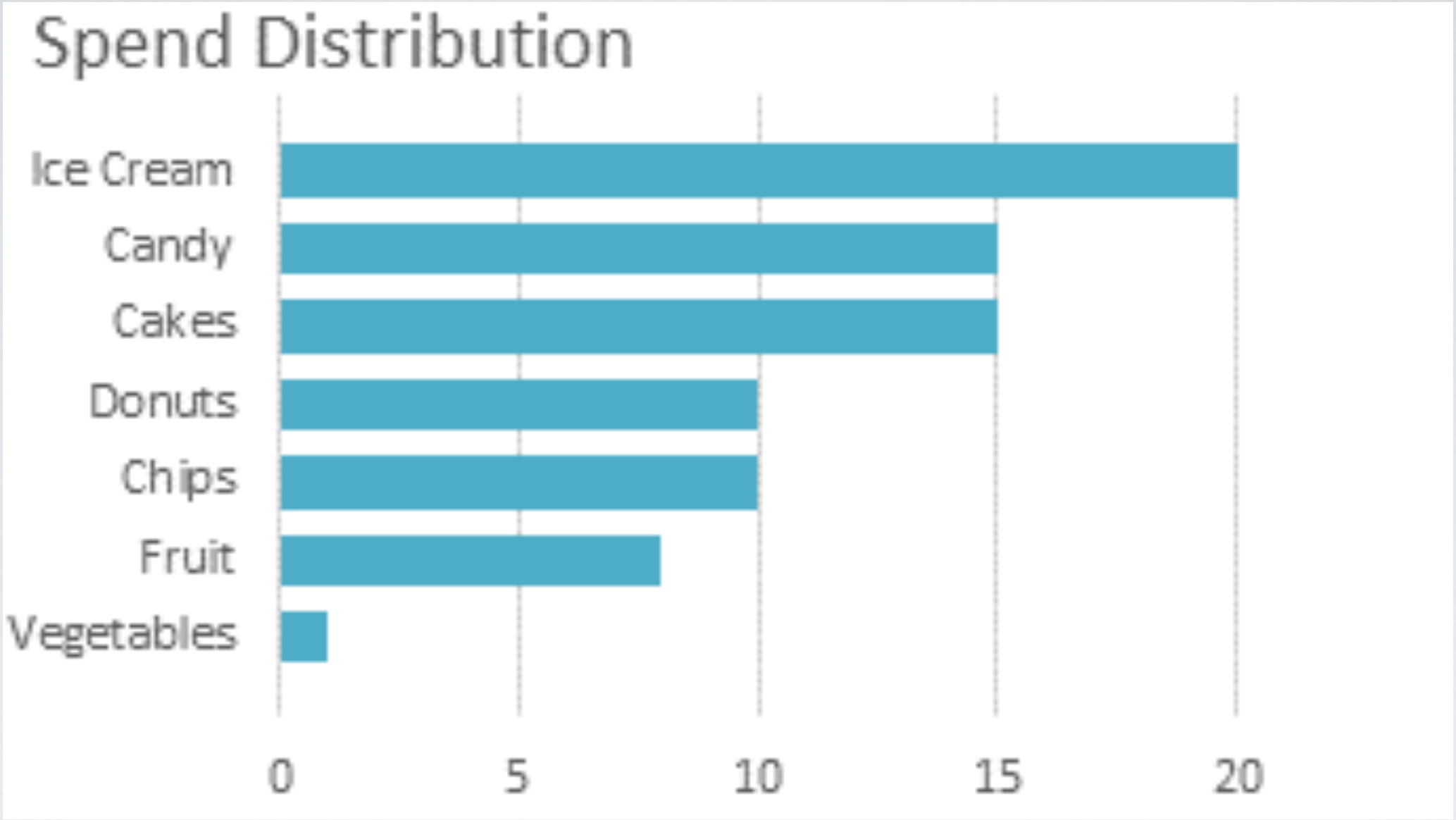
CLEVELAND'S HIERARCHY



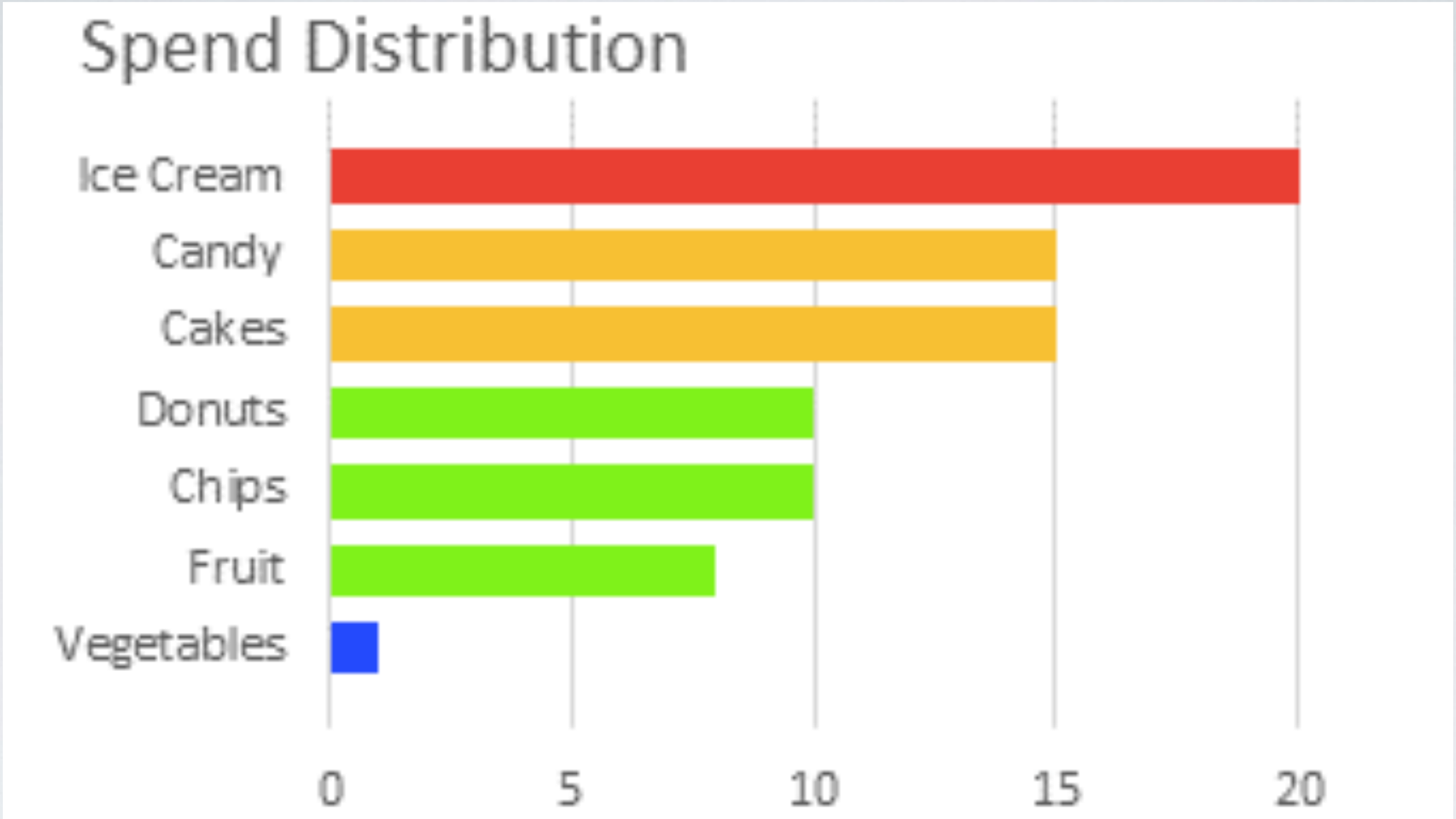
CLEVELAND'S HIERARCHY I



CLEVELAND'S HIERARCHY II



CLEVELAND'S HIERARCHY III



CLEVELAND'S HIERARCHY IV

POUŽITÉ TECHNOLOGIE V KYPO

- D3JS
- WebGL
- Liferay

D3JS

- dynamické a interaktivní vizualizace
- JavaScriptová knihovna
- HTML, SVG a CSS
- data-driven přístup

WEBGL

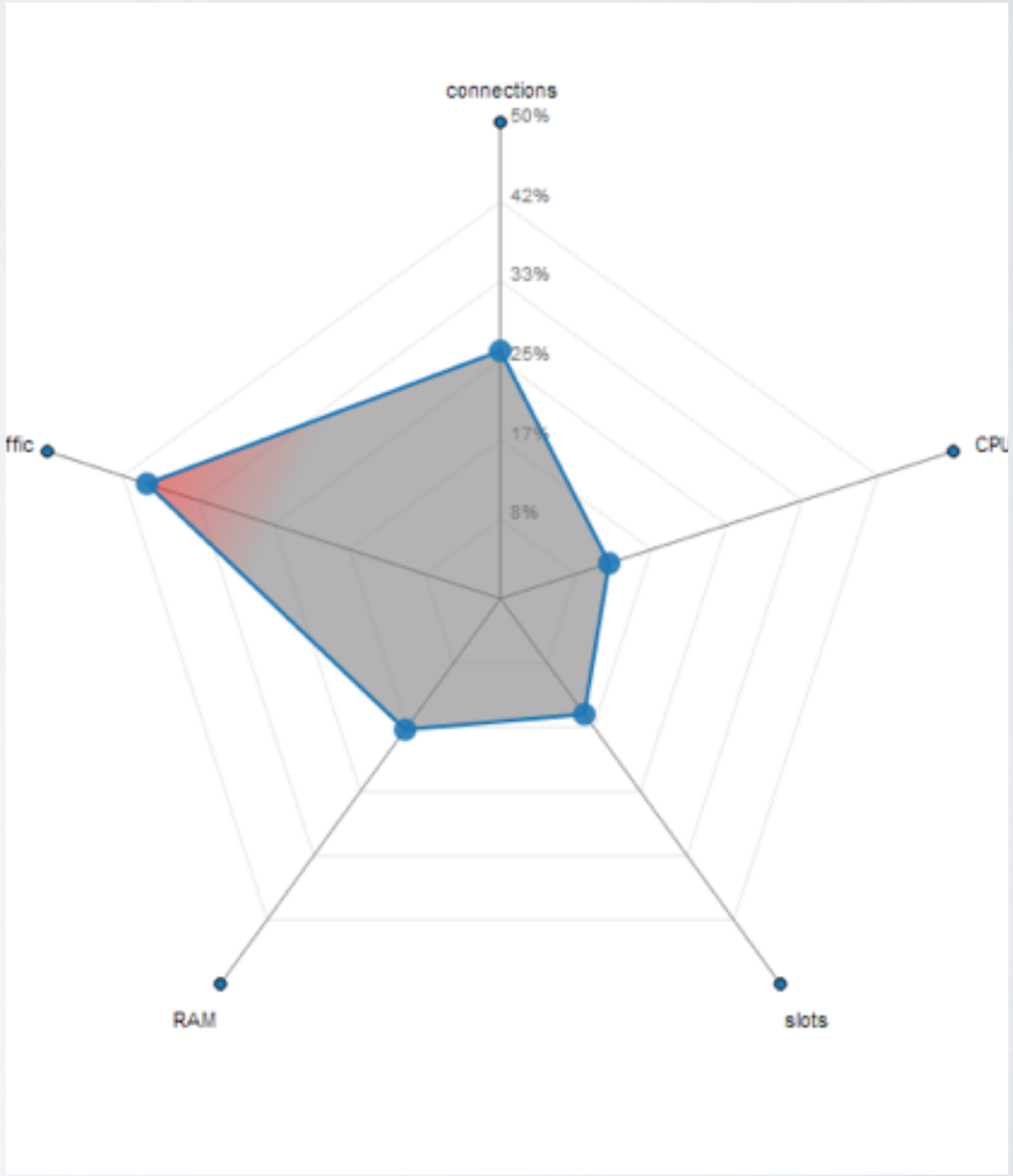
- JavaScript API
- výpočet na GPU klienta
- HTML5
- podporován všemi hlavními prohlížeči

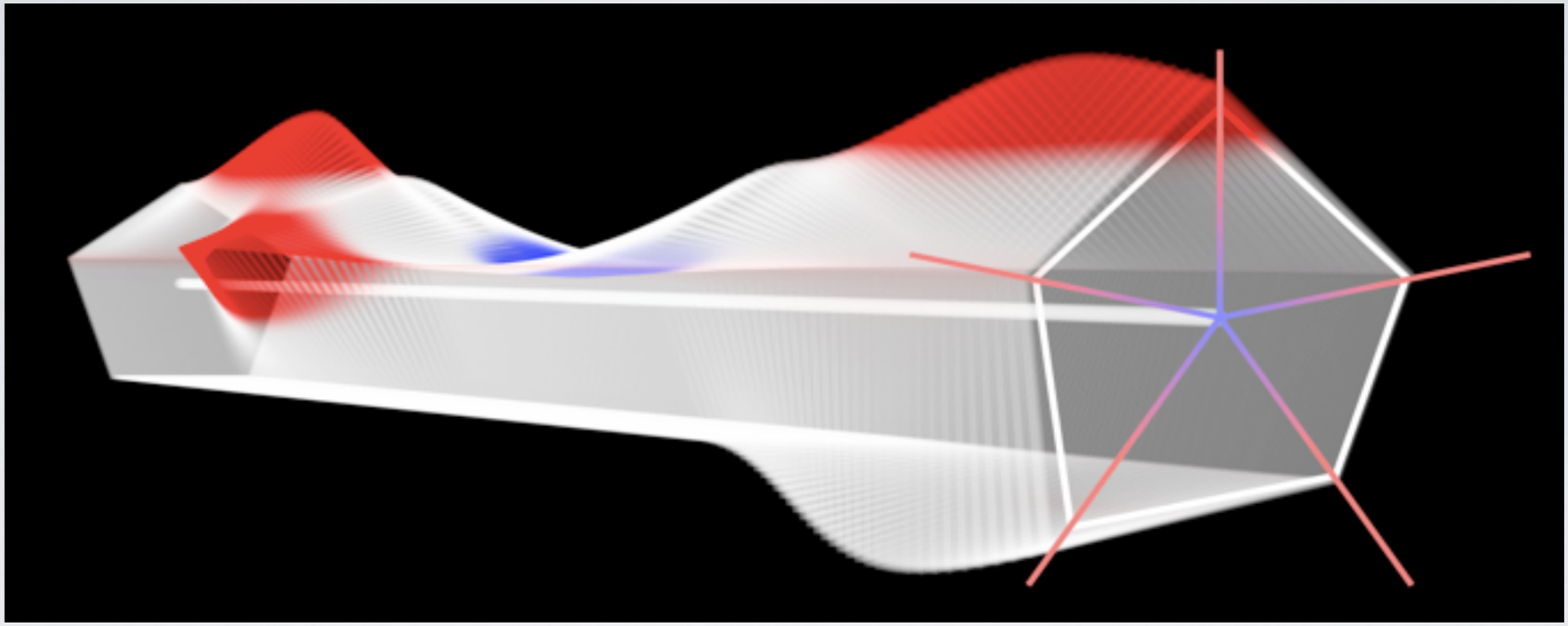
LIFERAY

- JAVA
- podnikový portál, skládá se z portletů
- módy portletu: VIEW, EDIT, HELP
- portlety mezi sebou komunikují

SPIDER CHART

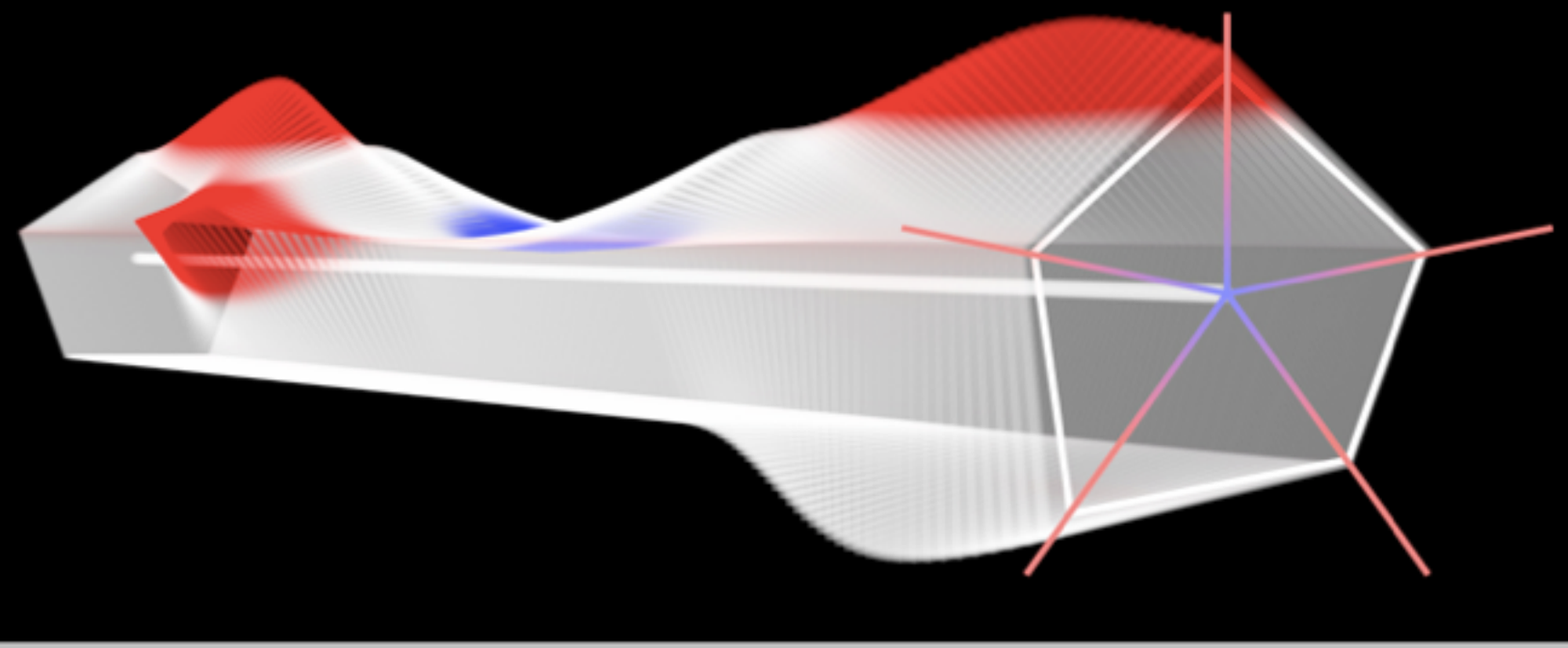
- 2D
- srovnání více proměných na jedné škále

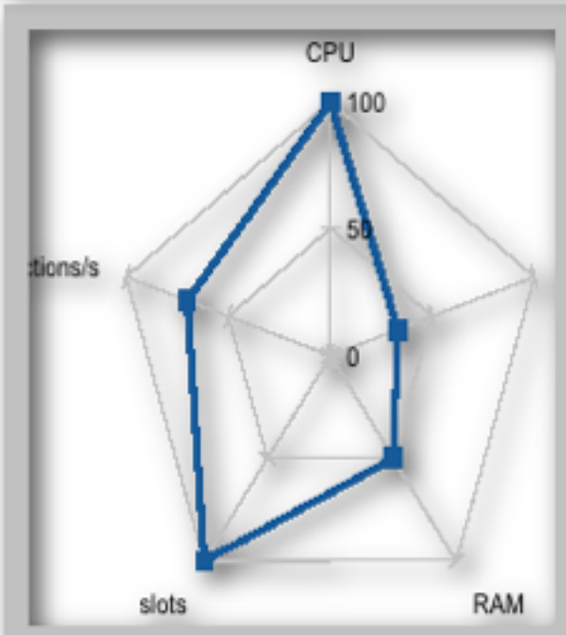




3D SPIDER CHART

NODE 11: EDIT

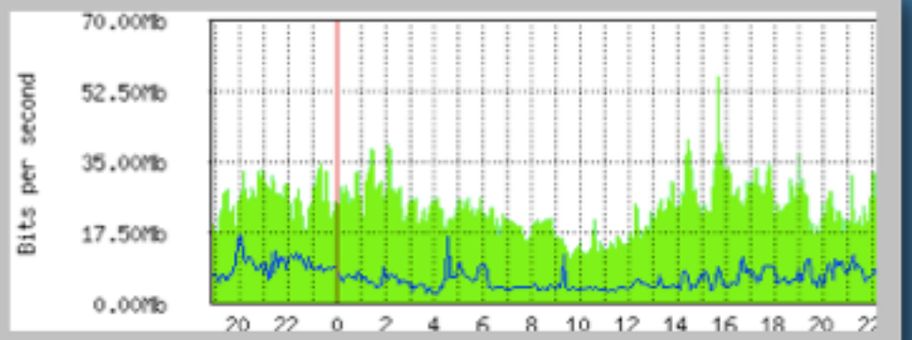


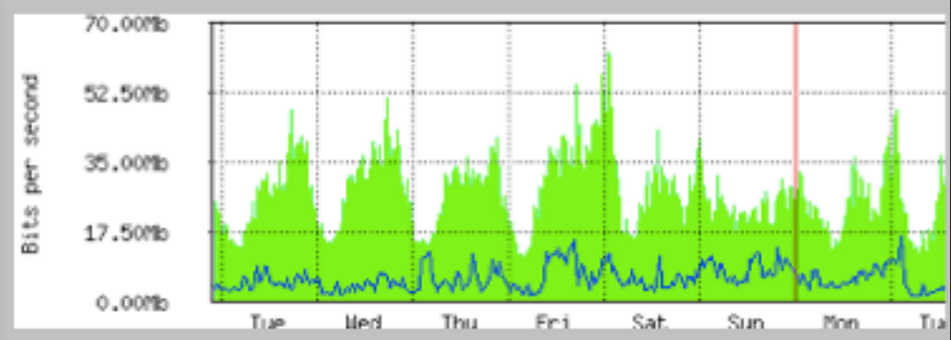


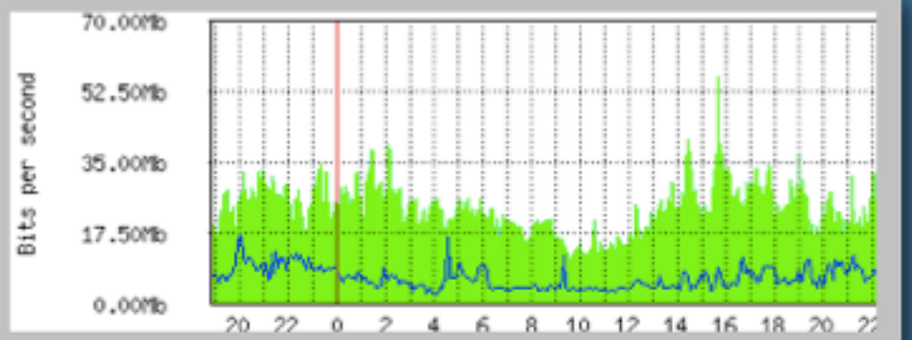
Overview

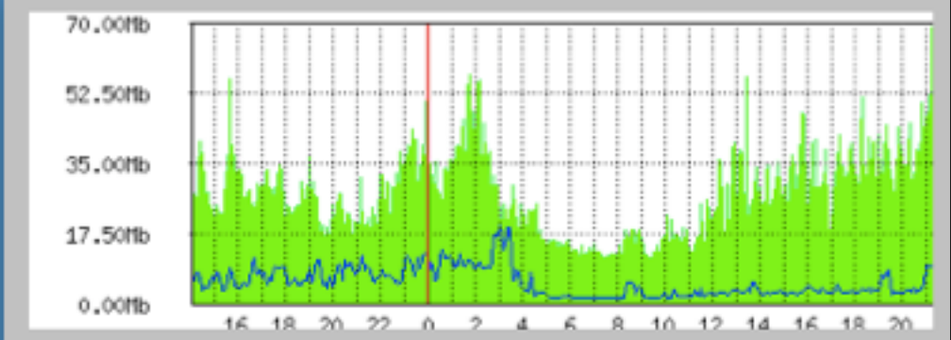
SYSTEM STATUS	RUNNING
SCENARIO	DDOS #1
NO. OF NODES	44
SYSTEM STATUS	RUNNING
SYSTEM STATUS	RUNNING

Node 11: EDIT









PRACOVIŠTĚ KYPO

LEAP MOTION