BSS469 Kybernetická bezpečnost

HISTORICKÉ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI

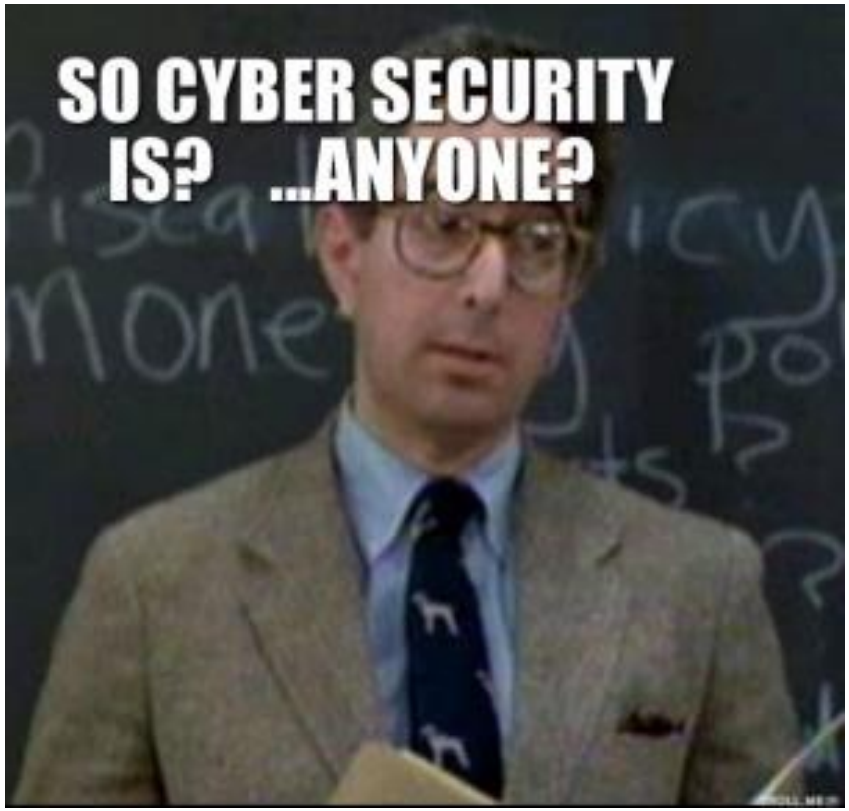
Daniel P. Bagge

National Cyber Security Centre

úvodem

- Exkurze na NCKB 27.10.
- Zašlete čísla OP na m.ulmanova@nbu.cz
- Předmět BSS469 – EXKURZE
- Celé jméno a číslo OP
- Do 10.10.2015

repetice



HISTORICKÉ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI

- Geneze kybernetických hrozeb, historie versus současnost
- Případové studie
- Taxonomie útoků, code based, content based (IW)
- Základní typologie a motivace útočníků

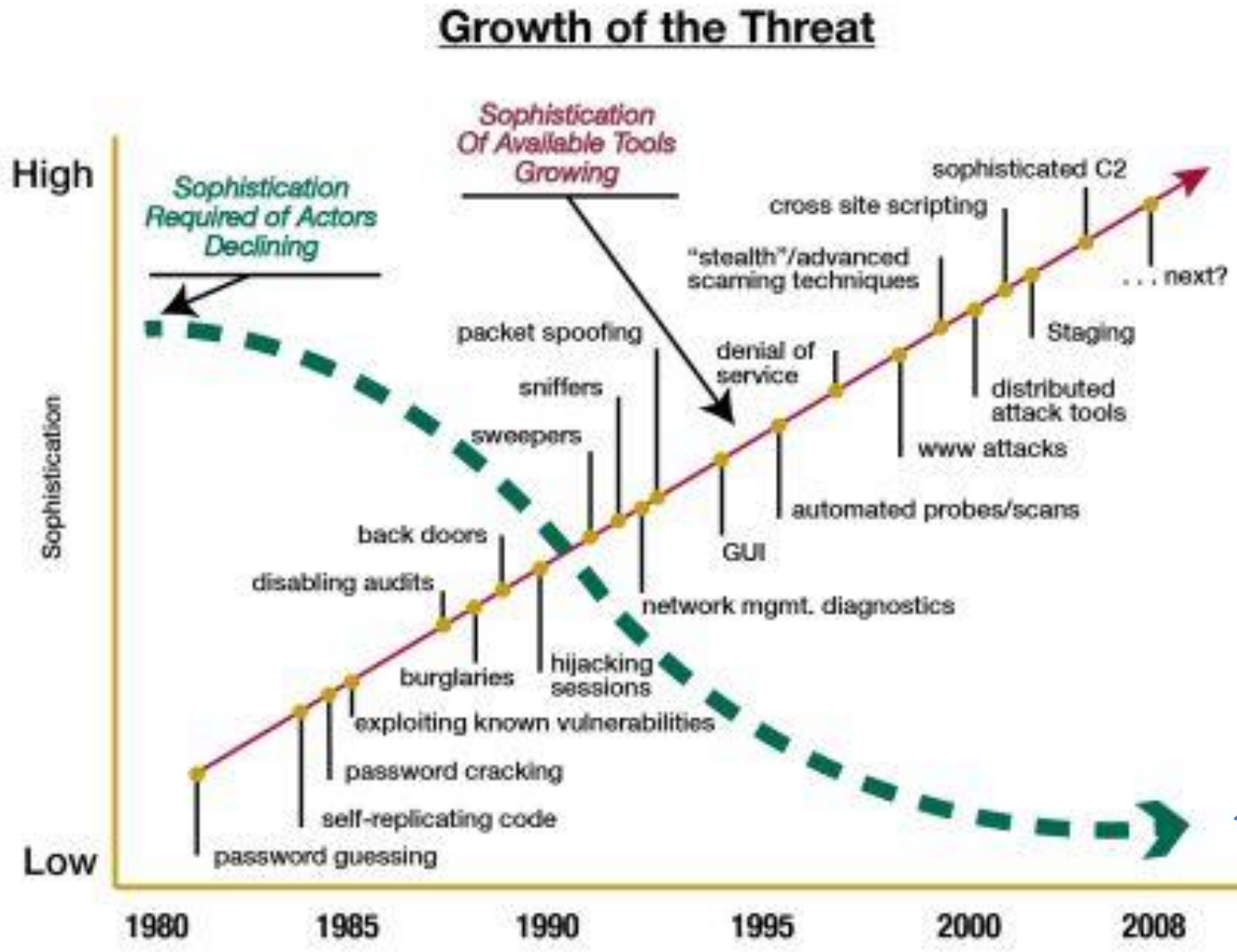
GENEZE KYBERNETICKÝCH HROZEB

- Cyber is dynamic and new
- Super fast, emerging TTPs every week, always changing
- If you woulkd like to understand it, and thus be secure you have to look forward – anticipate, be uncoventional, almost a futurologist
- No sense in looking back

GENEZE KYBERNETICKÝCH HROZEB

- Cyber i
- Super f changing
- If you v e secure you have to tional, almost a futurol
- No sen

GENEZE KYBERNETICKÝCH HROZEB



GENEZE KYBERNETICKÝCH HROZEB

- Cyber "Wake-up Calls"
  - Morris Worm
  - ELIGIBLE RECEIVER and SOLAR SUNRISE
  - MOONLIGHT MAZE
  - Chinese Espionage
  - Estonia and Georgia
  - BUCKSHOT YANKEE
  - OLYMPIC GAMES/Stuxnet

PŘÍPADOVÉ STUDIE

- **CUCKOO´s EGG**
- Hack U.S. DoE Lab /type Idaho, Livermore, Los Alamos
- Proxy entity/perpetrator from abroad
- Financed by foreign intelligence agency
- Targeted military R&D
- Compromised 40 military and governmental systems
- Honeypots, backtracing and international cooperation over 2 continents

PŘÍPADOVÉ STUDIE

- **CUCKOO´s EGG (1986)**
- KGB, CIA, FBI, NSA, AFOSI
- 1 scientist and 75 U.S. cents
- 4 men working as a proxy for the KGB
- Behavioral analysis of intruders
- More information
  - https://docs.google.com/file/d/0B_GtD5sFXOcCTkEyOXFy_X09qN2c/edit?pli=1
  - https://www.youtube.com/watch?v=EcKxaq1FTac

PŘÍPADOVÉ STUDIE

- FAREWELL DOSSIER
- 1 insider
- 2 presidents
- 4 intelligence/secret services of sovereign states
- Massive IP theft /years long campaign/
- Trojan horses implementation in hi-end technologies
- CII penetration and disruption

PŘÍPADOVÉ STUDIE

FAREWELL DOSSIER

- KGB, DST, CIA and others
- 4000 files
- Microchips, semiconductors, ICS/SCADA
- STUXNET style in 1982
- 3 KT of TNT?

PŘÍPADOVÉ STUDIE

- Shamoon
  - RasGas (Qatar) Saudi Aramco (SA)
  - Logical error in coding/scripts– amateur employee?
  - 30k to 55k compromised/affected computers/servers
  - Source – on the shelf and internet fora
  - Aramco partners?
  - No ICS impact
  - Aim – disruption/destruction,
  - Lowscale op, largescale impact

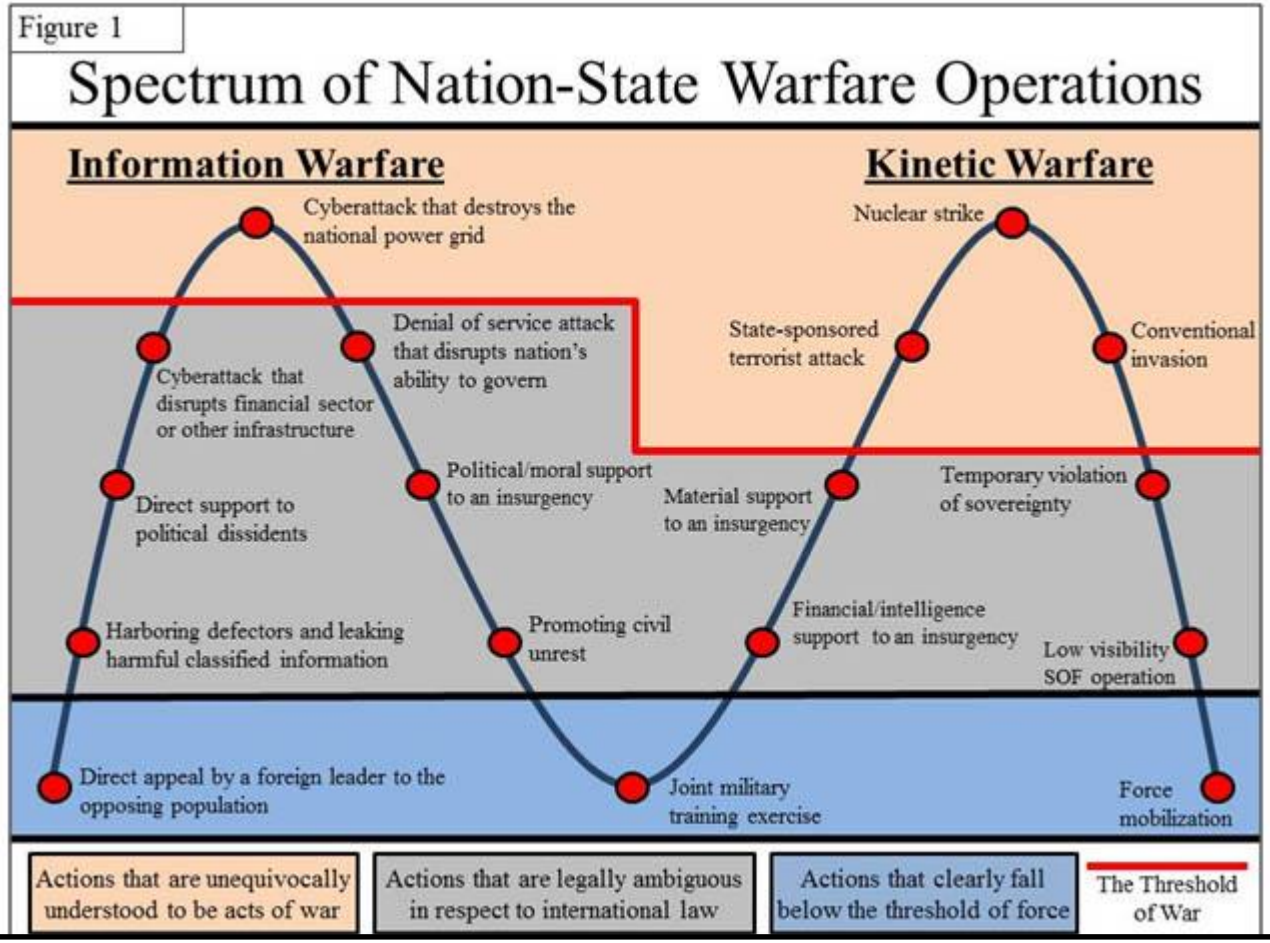
PŘÍPADOVÉ STUDIE

- Careto
  - Active since 2007 until January 2014
  - Highly modular (Vupen exploit 2012)
  - OpSec on unprecedented level
  - Platforms affected – Win, MacOS, Linux
  - Source – linguistic analysis, esp,port – narco?
  - Systems compromised in at least 31 countries

PŘÍPADOVÉ STUDIE

- Cuckoos egg and CARETO
  - 4 hackers, 1 astronomist, 75 U.S. cents
  - Highly sophisticated op sec, 7 years operational, world class capability
- Farewell and Shamoon
  - Fake SW and components manufacturing, years to carry out
  - 1 day – 30k - 50k computers

GENEZE KYBERNETICKÝCH HROZEB



http://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare

PŘÍPADOVÉ STUDIE

- http://map.norsecorp.com/v1/

GENEZE KYBERNETICKÝCH HROZEB

TAXONOMIE ÚTOKŮ, CODE BASED, CONTENT BASED

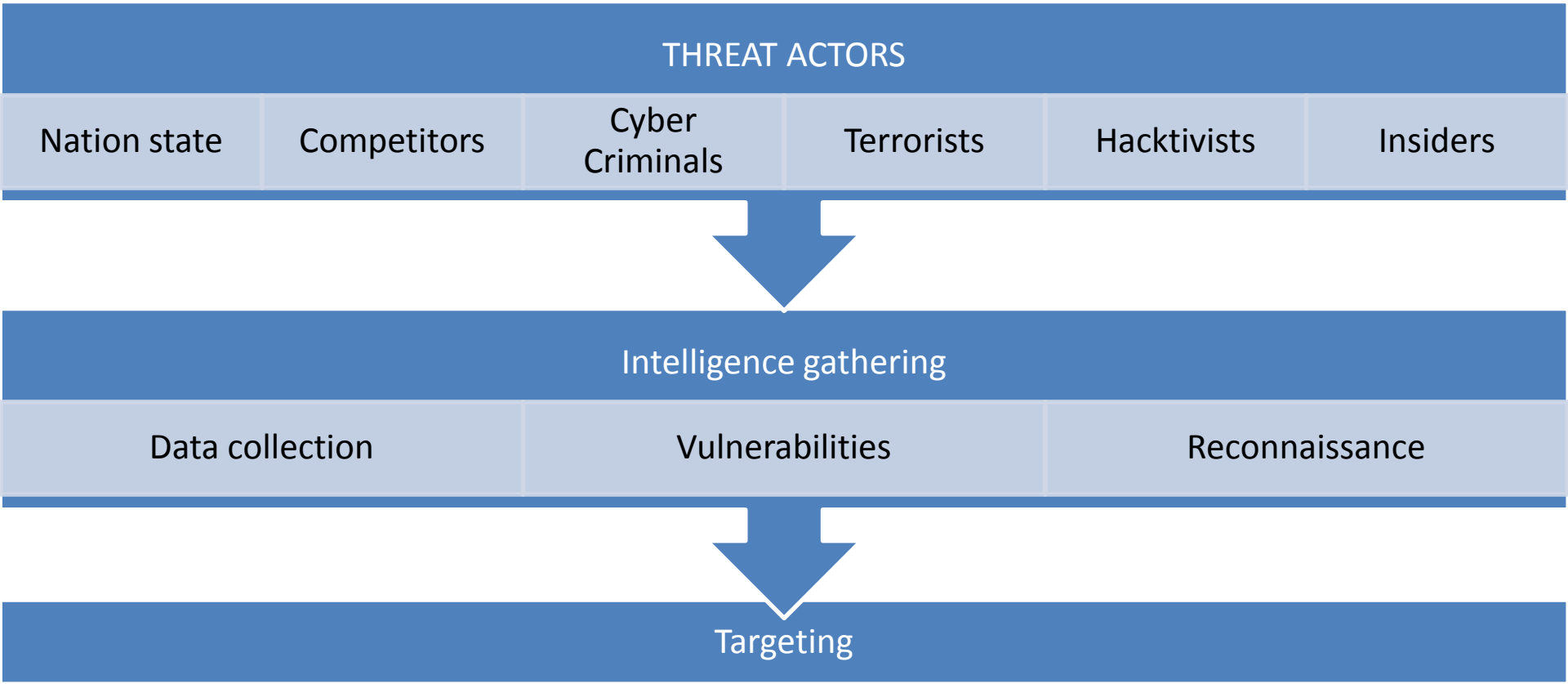
- Advanced persistent threat
- Distributed Denial of Service
- Cross-Platform Malware (CPM)
- Metamorphic and Polymorphic Malware
- Phishing
- Content based „hacking“

TAXONOMIE ÚTOKŮ, CODE BASED, CONTENT BASED

- Attack patterns
  - Crimeware
  - Insider and privilege misuse
  - Physical theft and loss
  - Web app attacks
  - POS intrusions
  - Payment card skimmers
  - Misc

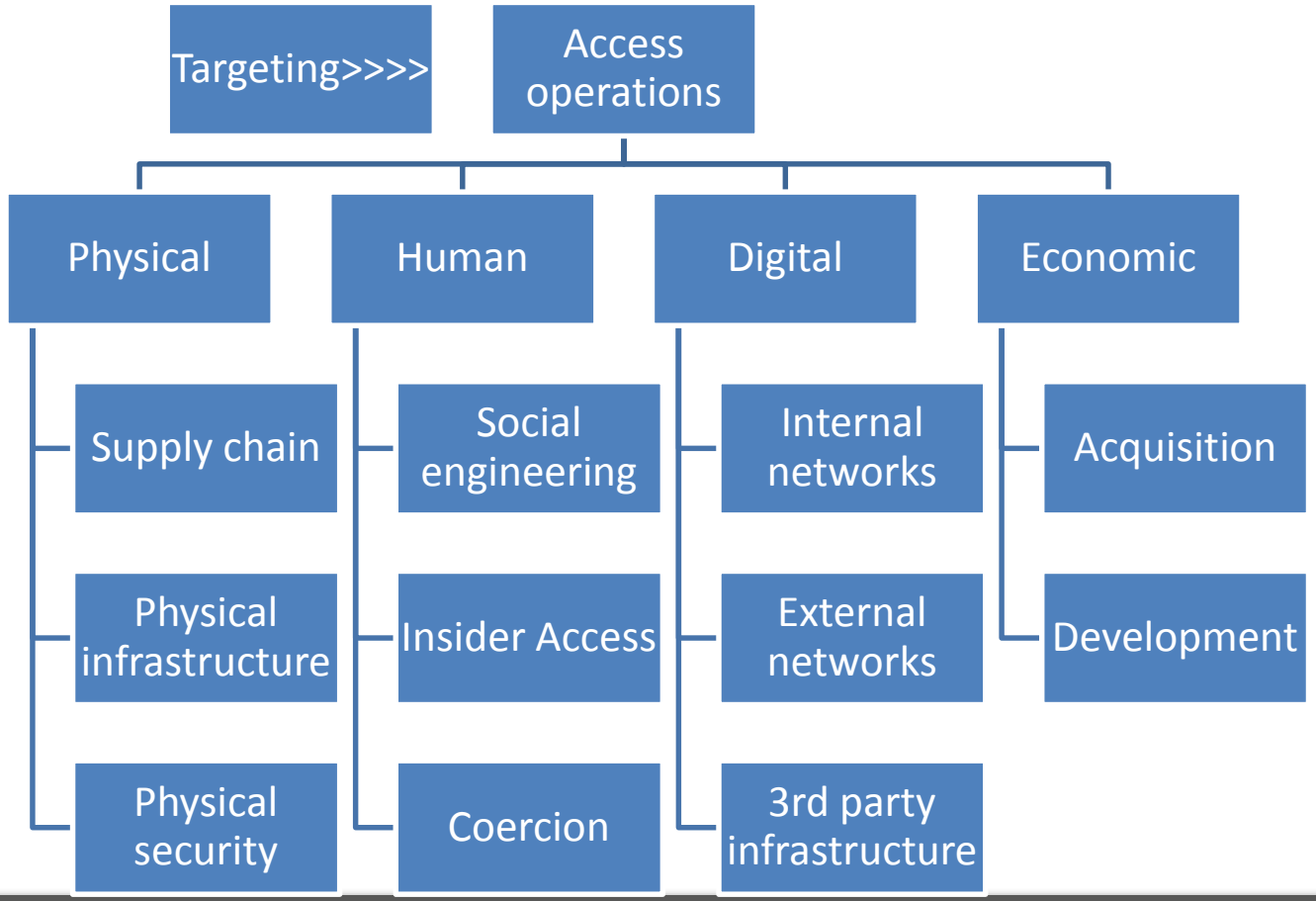
ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- Threat Actors – lines of work
  - Intelligence, Access, Offensive activities/Intrusions



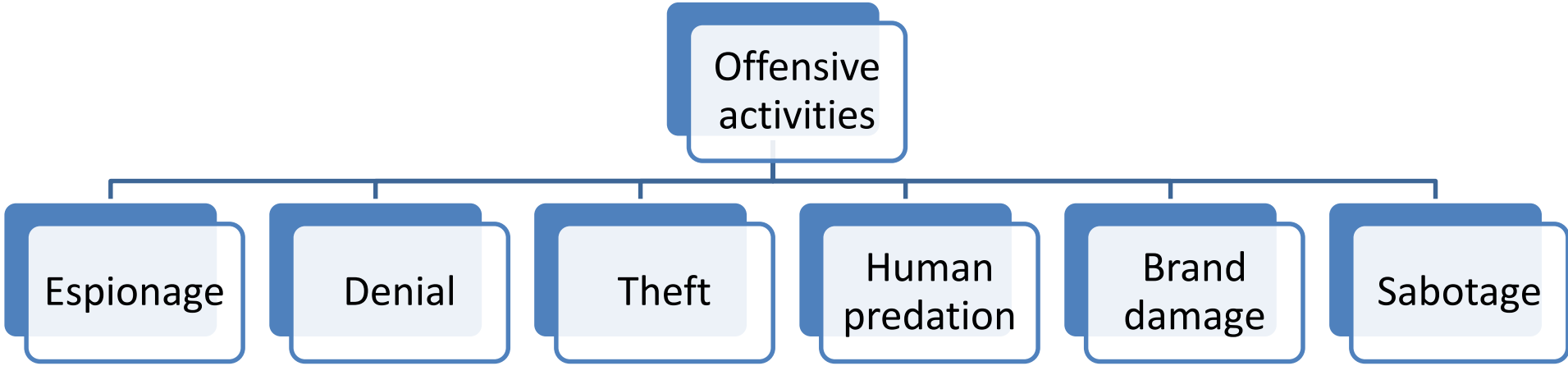
ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- Threat Actors – lines of work



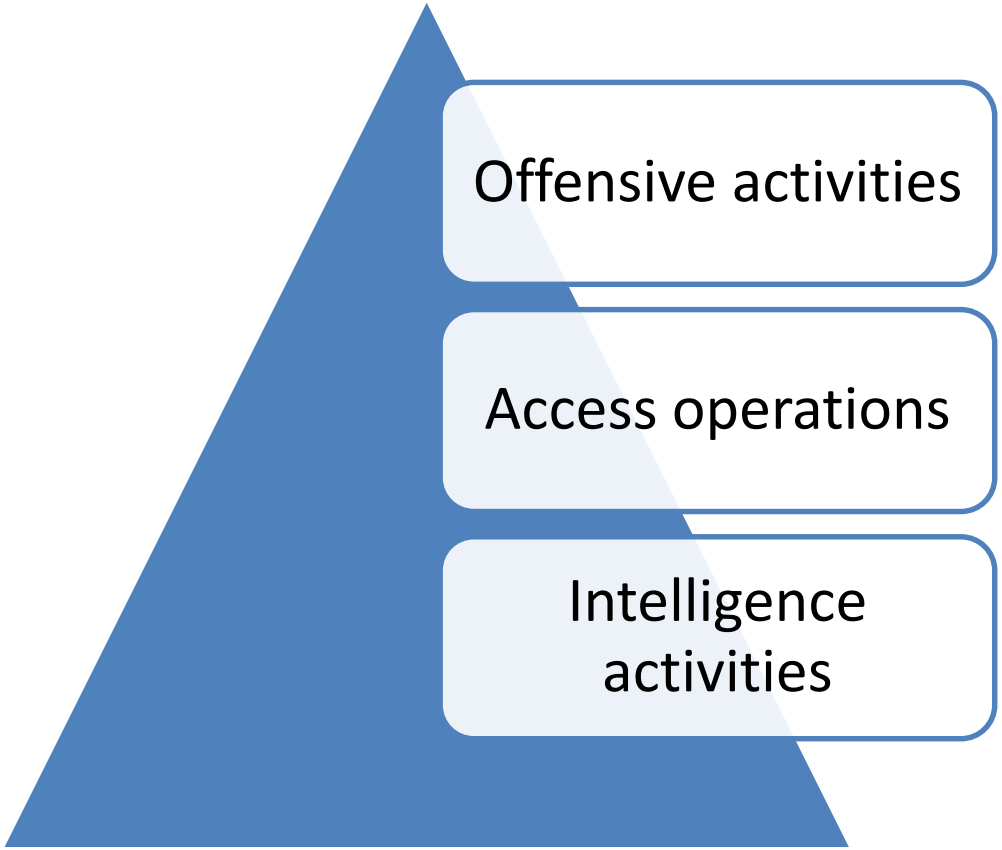
ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- Threat Actors – lines of work

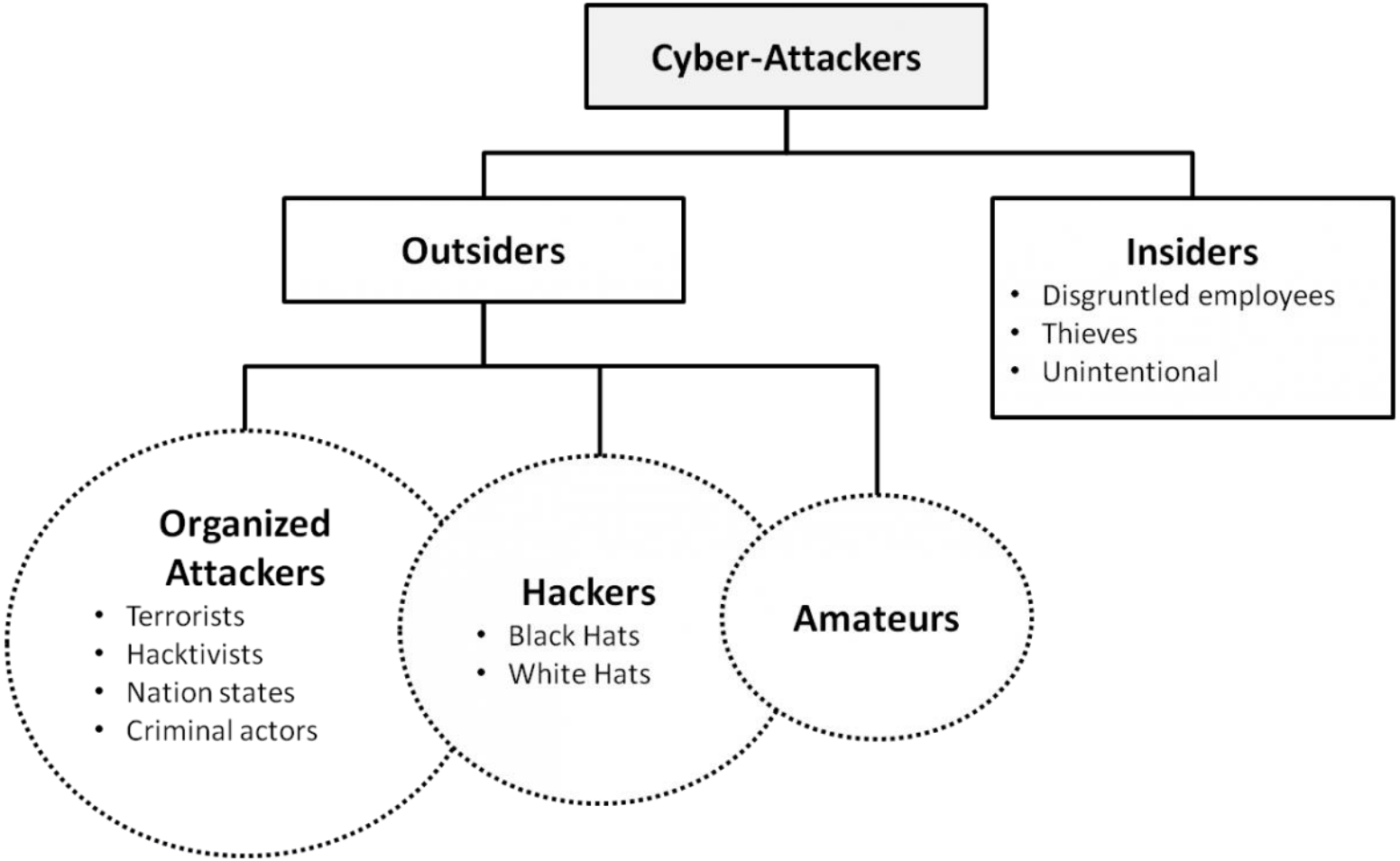


ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- Threat Actors – lines of work - summary



ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ



http://timreview.ca/article/838

ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- Hacktivist
  - Political gains/points
  - Anon, SEA?
    - Common attributes:
      - Ability/will to capture media attention
      - Bold, ambitious, recognizable aesthetics
      - Participatory openness
      - Surrounding misinformation
      - Unpredicatability

ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- Hacktivist
  - Anonymous
    - Splinter formations tech/nontech
    - From street protests to DDoS
    - Limited financial resources and skill sets / taking false credit
    - Elusive / unpredictable for threat intelligence
    - Ops usually linked to IRC channels/Twitter accounts
    - Socio political fabric – temporary unrest, hijacked brand

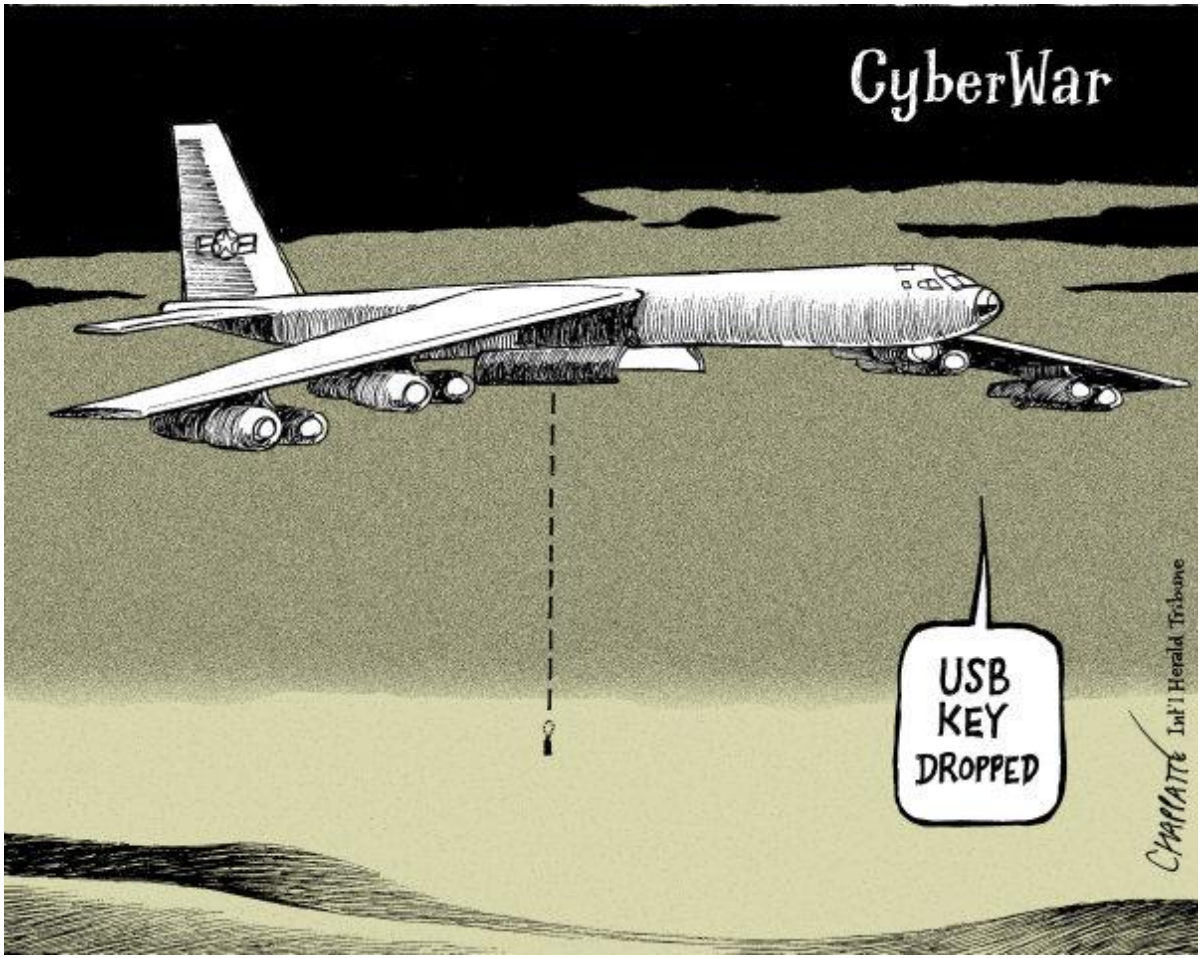
ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- Hacktivist
  - Syrian Electronic Army
    - Loyal hacktivist group to Bashar Al-Assad
    - Sophisticated attacks
    - Not limited to pro-gov activities
    - State sponsorship likely
    - Domain name of SEA – Syrian Computer Society, headed by Bashar
    - Toolkit – spear phishing, malware, remote access tools, trojans

ZÁKLADNÍ TYPOLOGIE A MOTIVACE ÚTOČNÍKŮ

- State sponsored entities
  - Backed by govs
  - Highly sophisticated, but not always
  - Well funded, high skill set

The End.



d.bagge@nbu.cz

National Security Authority