Improving Cybersecurity through Non-Technical Exercises and In-House Strategic Analysis

View from the Czech Republic

by Michal Thim

DISCLAIMER: *The views and opinions expressed in this presentation are those of the presenter and do not necessarily reflect the official policy, position of the National Cyber and Information Security Agency of the Czech Republic, or any other government agency.*

MICHAL THIM

- Cyber and policy/OSINT specialist at the Czech National Security Authority/National Cyber and Information Security Agency (NCISA) since August 2016, with research focus on East Asia (military and security developments, APTs)
- Background in political science. Not even remotely close to be a technical expert.
- Worked in a foreign policy think-tank (experience with decision-making environment)
- Tried academic environment (and left it behind, which made both me and academia quite happy)
- Developed some knowledge of Chinese language (can order coffee in Starbucks and has a 50% chance to answer correctly YES/NO question)
- Above is not atypical personnel profile at the NCISA

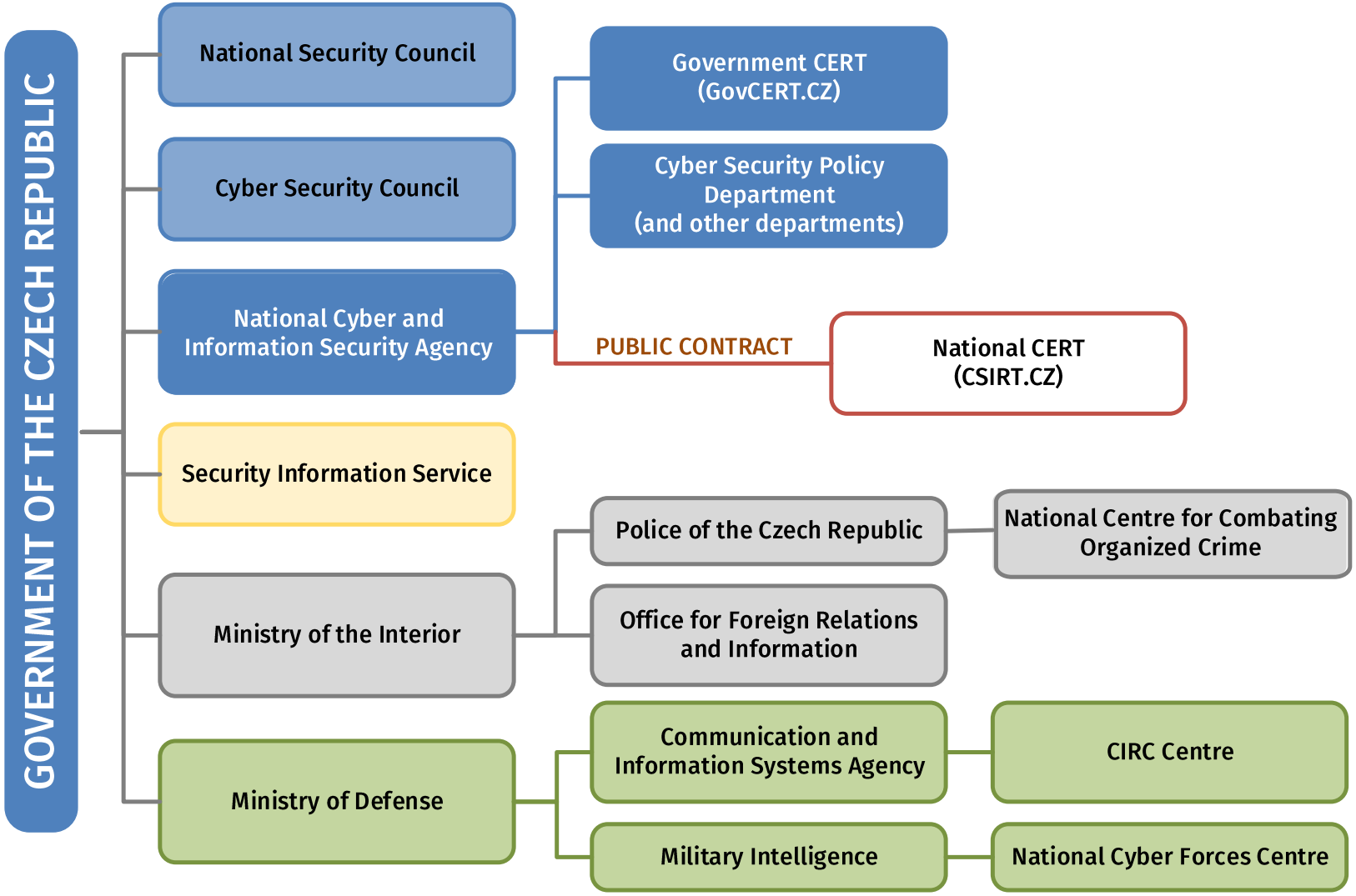
NATIONAL CYBER AND INFORMATION SECURITY AGENCY (NCISA)

- **Central body of state administration for cyber security**
- Mission(s)
  - Operation of the government CERT team: GovCERT.CZ
  - Cooperation with national & international CERT teams
  - Coordination and implementation of the National Cyber Security Strategy and related Action Plan
  - Protection of critical information infrastructure and other important systems (helping them to protect themselves)
  - **Preparation of exercises and education projects**
  - **Analysis and monitoring of cyber threats**
  - International cooperation

CONTENT

- Outline of the institutional framework for cybersecurity in the Czech Republic
- Non-technical exercises and its relevance for decision making process
- Strategic analysis helps decision makers to understand cybersecurity

CYBER SECURITY IN THE CZECH REPUBLIC: INSTITUTIONAL FRAMEWORK (1)



CYBERSECURITY IN THE CZECH REPUBLIC: INSTITUTIONAL FRAMEWORK (2)

- Even relatively simple setup involves number of agencies across government sector
- There is a significant number of people that need to be well-informed, so they make the right decision in a timely fashion when the crisis comes.
- One way: cyber security exercises that simulate real-world possibilities
- Another way: strategic analysis

A FEW GENERALIZATIONS

Policy and decision makers

- Strategic perspective
- Have direct (political) responsibility for policy decisions
- Need to take into considerations inputs from various directions, including domestic and international law
- Do not always understand severity of a cyber security incident

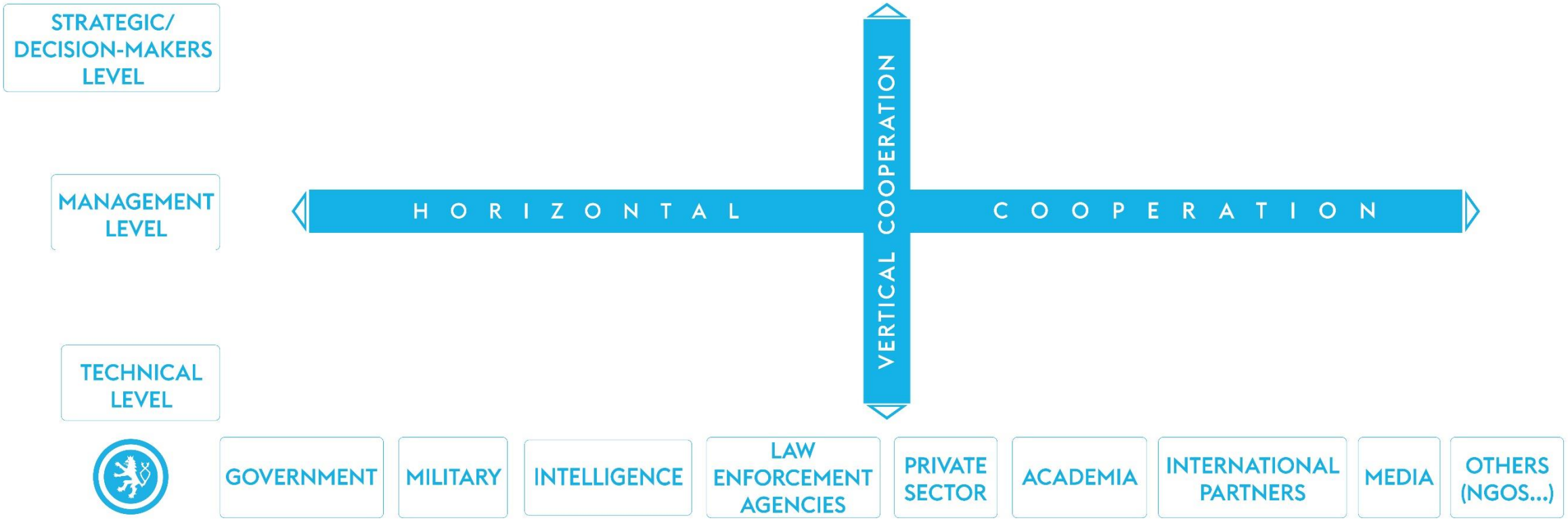
Technical experts

- Operational/tactical perspective
- Specialists in their respective fields
- See decision making as slow, not corresponding to pressing needs
- Do not always communicate with decision makers in a mutually understandable manner

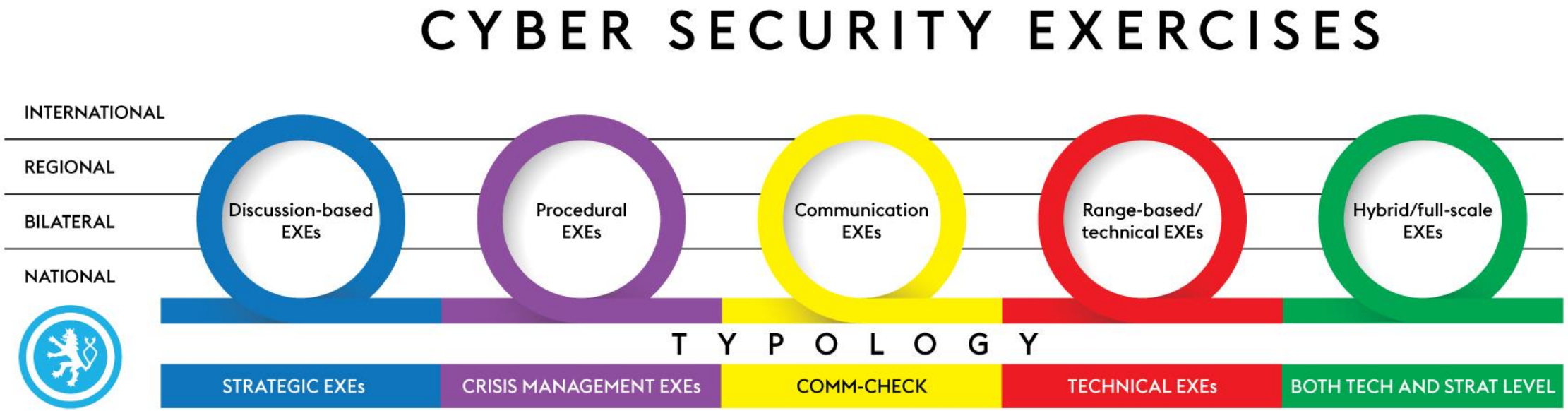
EXERCISES TYPOLOGY

1. COMM-CHECKS
   - Testing existing/stated communication channels
2. **STRATEGIC EXERCISES (incl. tabletops)**
   - **Real world-like scenarios, crisis simulation**
   - **We do customized TTXs for partners (e.g. U.S. Cyber Command, NATO ACT)**
3. CRISIS MANAGEMENT EXEs (CMXs)
   - Specifically designed to test existing decision-making processes
4. TECHNICAL EXERCISES (Cyber ranges)
   - Simulated attacks, Red team Vs Blue team
5. **HYBRID/FULL-SCALE EXEs**
   - **Exercises involving technical and non-technical elements (not necessarily integrating them)**
   - **Provides link between technical teams and strategic perspective**

EXERCISES TYPOLOGY



EXERCISES TYPOLOGY



LOCKED SHIELDS 2017

LOCKED SHIELDS

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

NÚKIB

LOCKED SHIELDS 2017

- Coordinated by Cooperative Cyber Defense Centre of Excellence (CCDCOE) based in Tallinn, Estonia
- Since 2010
- Participants in the exercise are NATO member states, NATO partner countries & NATO CIRC team (possible Australian participation in future?)
- Four teams (up to 200 personnel] operate out of Tallinn, Estonia:
  - RED TEAM
  - GREEN TEAM (physical and online infrastructure)
  - WHITE TEAM (scenario)
  - YELLOW TEAM (operational awareness)
- BLUE TEAMS operate out of their respective countries
- 19 blue teams took part in LS17
- Czech team participated in preparation and was involved in white, red and green teams
- Czech blue team: NCISA, CZ.NIC, MoD and others

LS17: SCENARIO

- Blue teams assumed role of government CERT teams of a fictional country Berylia
- Red team assumed role of a fictional country Crimsonia that has a long-standing dispute with Berylia and generally considers it as partr of its influence sphere
- Target:
  - Major air base
  - Control of Unmanned Aerial Vehicles crucial for Berylia's defense and domestic industry
  - Fuel storage (SCADA systems)
- Blue teams were scored not only based on their ability to keep their systems operational, but also in terms of how they reacted to **media AND legal queries**

STRATEGIC GAME AT LS 2017

- Based on the same scenario but included some extras: cyber attacks on elections that preceded the technical game scenario
- It was not strictly speaking strategic game because no high-ranked personnel was involved
- Blue teams had to consider their own legal/institutional frameworks and take decision their governments would take
- Few lessons:
  - Legal aspects are important, especially if the conflict has international nature (international law, Tallinn Manual 2.0)
  - The existing legal and institutional frameworks are often not ready to deal with effects of cyber attacks
  - It is relatively easy to overreact/underreact

LOCKED SHIELDS 2017

Czech Team Wins Cyber Defence Exercise Locked Shields 2017

The team from Czech Republic wins the largest and most complex international live-fire cyber defence exercise Locked Shields 2017. Estonian team and NCIRC team from NATO take second and third place respectively.

The defensive team from Czech Republic also takes home the special prize for the scenario inject. NCIRC team scored the highest in the legal game of the exercise, German team came out on top of forensic challenges while the team from the United Kingdom achieved the highest scores in handling the strategic communication challenges.

"The winning team demonstrated that good tactics and stable performance in all categories can lead to best overall scores in the end. The experts of the Czech team performed also very well in the strategic track that was a new addition this year," highlights Aare Reintam, Technical Exercise Director at NATO CCD COE.

CYBERCZECH 2016 TTX

NÚKIB

CYBERCZECH 2016 TTX

- Tabletop exercise (tabletop version of technical CyberCzech exercise)
- scenario involved fictional countries of Pilsneria, its ally Brotherland, and Sauronia that declared “cyber war” on Pilsneria
- loosely based on civil war in Syria and European refugee crisis
- Events (and injects) involved:
  - DDoS attacks, data theft, theft of laptop, ransomware attacks, attacks on power grid, UAV hijacking…full menu, really
- Combination of cybersecurity incidents/attacks and physical domain events
- 6 teams: public servants, intelligence community and military, legal team, decision-makers, private sector, media => NOT SIMULATED

CYBERCZECH 2016 TTX

Lessons learned included:

- Decision-makers hesitate to act
- Media communication is essential
- Need for greater emphasis on cyber hygiene (theft of laptop part of scenario, email habits exposed participants to spear-phishing)
- Technical and non-technical teams need to communicate clearly with decision makers
- Greater emphasis on whole-of-society approach (e.g. MIL hesitated to cooperate with CIV)
- Briefings on strategic level are inadequate and mostly reactive

STRATEGIC ANALYSIS AT NCISA

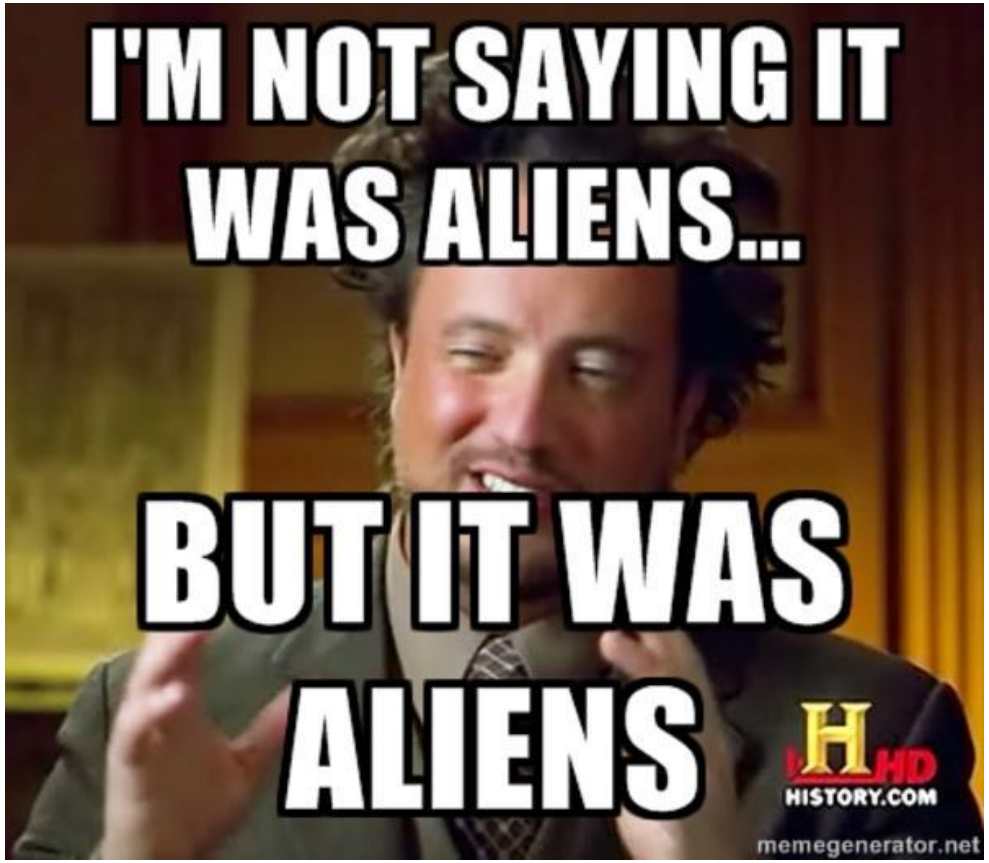
- OSINT-based (Open-Source Intelligence)
- Early warning system
- Risk prevention
  - prevention of cyber threats and future attacks through context analysis
- Information support during crisis situations
- Knowledge base build-up (collection of resources, own analytical production)
- Information sharing

NCISA BE LIKE...

- Combine open source and Government CERT information (or in more general terms: combine knowledge of technical and non-technical teams)
- Not all strategic analysis at NCISA is a result of cooperation between OSINT team and GovCERT nor is there a need for it
- We know we can reach out to each other anytime

STRATEGIC ANALYSIS

```
if ( !CryptAcquireContextA(&hProv, 0, "Microsoft Base Cryptographic Provider v1.0", 1u, 0) )
{
  if ( GetLastError() != -2146893802 )
  {
    free(v7);
    return 0;
  }
  if ( !CryptAcquireContextA(&hProv, 0, "Microsoft Base Cryptographic Provider v1.0", 1u, 8u) )
  {
    free(v7);
    return 0;
  }
}
if ( !CryptImportKey(hProv, &Key, 0x94u, 0, 0, &hKey) )
{
  free(v7);
  if ( hProv )
    CryptReleaseContext(hProv, 0);
  return 0;
}
*(_DWORD *)v7 = 0;
v9 = 0;
v10 = v7;
if ( fOAEP )
{
  while ( 1 )
  {
    v11 = v9 + 117 >= v6 ? v6 - v9 : 117;
    pdwDataLen = v11;
    memcpy(v10, (char *)hCrypto + v9, v11);
    v9 += pdwDataLen;
    if ( !CryptEncrypt(hKey, 0, 0, 0, (BYTE *)v10, (DWORD *)&pdwDataLen, 0x80u) )
      break;
    v10 = (char *)v10 + pdwDataLen;
    if ( v9 >= fOAEP )
    {
      v7 = v15;
      goto LABEL_12;
    }
```



SYNERGY OF TECHNICAL AND STRATEGIC ANALYSIS

- Still relatively new
- ThreatConnect & DGI cooperation on an exposure of Unit 78020 is a very good example
- Governments have the choice to outsource but for many reason they will often opt to do it in-house
- The advantage is that the cooperation becomes institutionalized over time and not just ad hoc/project-based
- Strategic analysis informed by technical analysis supports good decision making

HOW NON-TECHNICAL EXERCISES IMPROVE CYBERSECURITY?

- Confront decision makers with life-like situations
- Involves personnel that is typically not a part of a technical exercise
- Allows to employ scenarios that reflect real-life events: helps decision makers to go from abstract to practical aspects of cybersecurity incidents
- Demonstrate that events in cyberspace could lead to physical damage and/or exploit pre-existing division in society
- It is a learning lesson for all involved
- Principals lead by example if they take part (reality: they tend not to do it)
- Clarification of roles
- Networking

FEW REALLY FINAL WORDS

- Much has been said about the role of exercises and strategic analysis and how they help to bridge communication between technicians and decision makers
- Not much has been said about people who are preparing exercises and relaying communication from technical/tactical to decision-making/strategic level
- We are not superheroes who came to save the day, the process is a great learning experience for everyone involved and that includes us


That's all Folks!

CONTACTS

@m.thim@nukib.cz

@michalthim

PGP: 0B31 F374 9C42 60FF 8182 19A7 4168 1972 DD10 E97E