STRATEGIC TABLE-TOP EXERCISES

Why are they so important for national resilience?

Martina Ulmanová

Head of Cyber Exercise Unit

Michal Thim

Specialist of Strategic Information and Analysis Unit

National Cyber and Information Security Agency

CONTENT

- Few words about us
- Have you ever..?
- Possible scenario background
- Domains and entities affected
- Challenges to address (a decision-making perspective)
- Solution: Strategic TTXs
- Czech experience with exercises
- Takeaways and observations

INTRODUCTION

Martina

- Background in security studies
- Work as a head of cyber exercise unit at the Czech National Cyber and Information Security Agency
- Have served as an exercise director and local trainer for NATO Cyber Coalition exercise
- Have been a member of EPG of Locked Shields exercise, in 2017 became a leader of scenario inject team

Michal

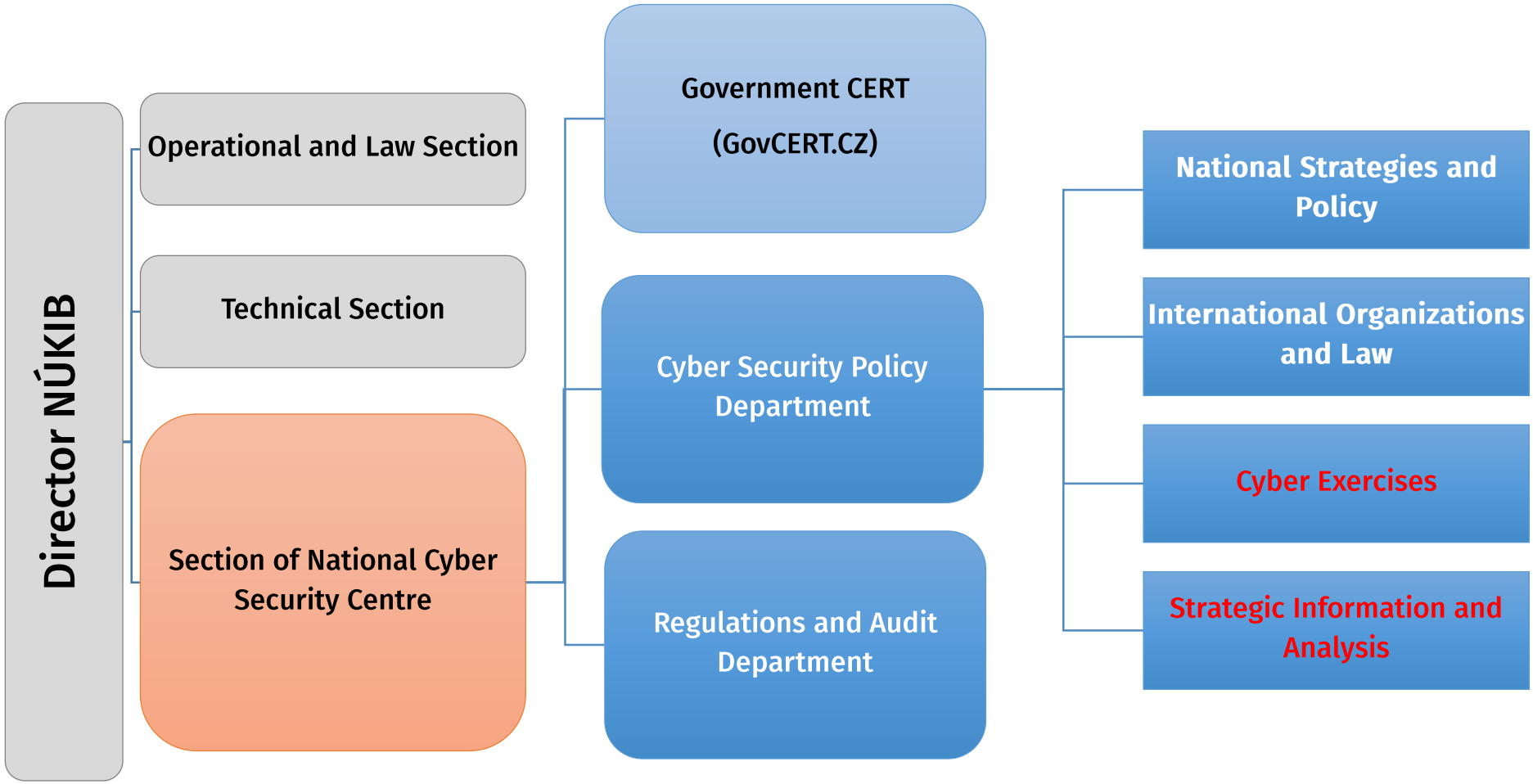
- Background in political science
- OSINT specialist at the Czech National Security Authority/National Cyber and Information Security Agency (NCISA) since August 2016
- with research focus on East Asia (military and security developments, APTs)
- Worked in a foreign policy think-tank (experience with decision-making environment)

NATIONAL CYBER AND INFORMATION SECURITY AGENCY (NCISA/NÚKIB)

- **National authority 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

NATIONAL CYBER AND INFORMATION SECURITY AGENCY (NCISA/NÚKIB)

NATIONAL CYBER AND INFORMATION SECURITY AGENCY (NCISA/NÚKIB)



FEW GENERALIZATIONS

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

So you have a CERT/national cyber authority.

So what?

HAVE YOU EVER….?

Information security researchers

Government employees

Computer Emergency Response Team members

Technical experts

Private sector representatives

Journalists

… and others that are present

participated in a TTX/tech exercise TOGETHER?

With the increasing profile of attacks and cyber security as a topic in general

the level of decision making gets higher, without having the involved decision makers trained or knowledgeable

HAVE YOU EVER….?

Who was the highest ranking official with no direct cyber responsibility to participate in a crisis/cyber exercise?

*no direct responsibility – deputy minister for national security, overarching executive powers, decision makers…

POSSIBLE SCENARIO BACKGROUND

- Cyber attack on an electrical grid (national level)
  - Real-world case
- *What could be the broader implications?*
- *Would you be ready for such an event?*

DOMAINS AND ENTITIES AFFECTED

- SCADA systems compromised - **technical aspect**
- Partial shortages at military base – **military aspect**
- Limited distribution of energy, outages - **national crisis impact**
- Massive overload abroad – **international/diplomatic aspect**

DOMAINS AND ENTITIES AFFECTED

- Multiple distribution vectors - **affected private sector**
- Millions citizens - **affected public, outrage**
- Communication crippled – **national/media matter**
- Intentional breach, existing conflict, sabotage - **national security matter**

CHALLENGES TO ADDRESS

- **GOV**
  - Do you have recovery plans for a large scale cyber attack?
  - Do you have policies in place, the necessary personnel?
  - What GOV department should be the lead in coordinating the investigation and countermeasures?
- **MIL / INTEL**
  - Would be the cyber attack, crippling the defensive capacities, considered as a use of force?
  - Is the military legally and operationally able to conduct active defence operations in peacetime conditions (IHL) in a possibly asymmetric campaign like this?

CHALLENGES TO ADDRESS

- **LEA**
  - Are the legal conditions for a declaration of state of emergency fulfilled?
  - Do you have legal framework to respond to a cyber crisis from an investigative/prosecution perspective? Who has the lead?

- **MEDIA / DIPLOMATIC**
  - How do you communicate your position to the citizens if they are out of power?
  - Do you have means for contacting the neighbouring country to remedy possible impact on their grid?

CHALLENGES TO ADDRESS (A DEC-MAK PERSPECTIVE)

- Cyber security requires a **multi-disciplinary approach with management participation**
- Imperative to have **significant number of individuals well-informed** to carry out the right decision at the right time
- **Cyber knowledge gap** (techies vs dec-maks, junior vs senior generation)
- **Responsibility can no longer be delegated** only to geeks in server room

CHALLENGES TO ADDRESS (A DEC-MAK PERSPECTIVE)

- **Lack of support** towards ICT depts from their superiors
- **Lack of leading** by example from top level
- Inability to build up and retain skilled teams, **problem with motivation**
- **Limited capacities** to educate individuals on a large scale and in a timely fashion (poorly trained workforce presents the greatest threat)
- **Focus on technology** vs underestimation on dec-mak level
- **Complicated bureaucratic system** vs dynamic nature of cyber threats

CHALLENGES TO ADDRESS (A DEC-MAK PERSPECTIVE)

- Do you think all these challenges are on the mind of the decision-makers?
- Are they aware of them?
- So where are the decision-makers from?
  - Tier 3 – Cyber
  - Tier 2 – National Security
  - Tier 1 – Political leadership

Cyber Defence

Critical Information Infrastructure Protection

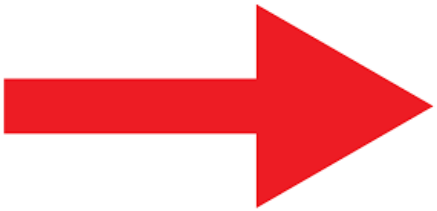
Cyber Crimes

Intelligence Services

RESILIENCE IS DEPENDENT ON THE ABILITY TO ACT

- Do you think the leaderships of the previously mentioned entities are on the same page? (and not taking in account academia and private sector and the constituency)
- **Absolutely not. WHY?**
  - different mandates
  - different missions
  - different interests
  - different capacities/resources
- **How can GOV be able to react dynamically and efficiently?**

Cyber security is not just a technical issue, it is an executive-level concern



SOLUTION: STRATEGIC LEVEL CYBER EXERCISE

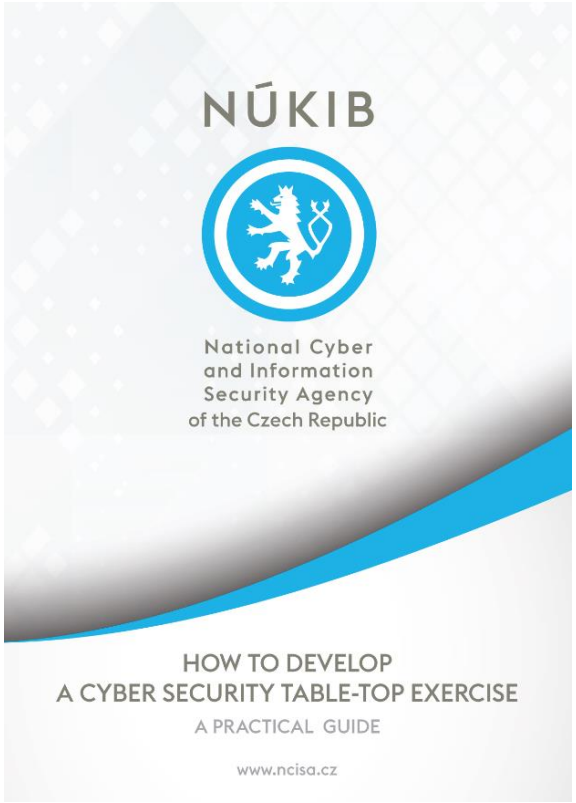
- Exposure of senior leaders to cyber
- Low cost - high impact
- Active involvement of the audience
- One exercise - various challenges/training objectives

SOLUTION: STRATEGIC LEVEL CYBER EXERCISE

- High stress simulation – behaviour in crisis situation
- Two-way learning process
- Multiple execution
- Helps to go from abstract to practical aspect of cyber
- It is a learning lesson for all involved

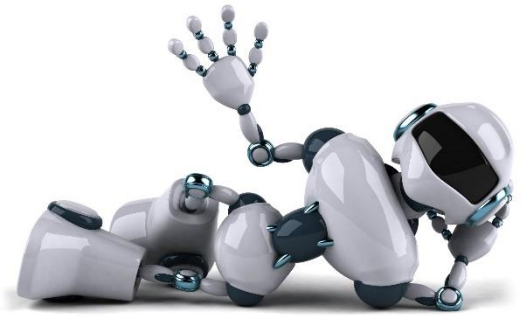
CZECH VIEW: WHAT IS NECESSARY

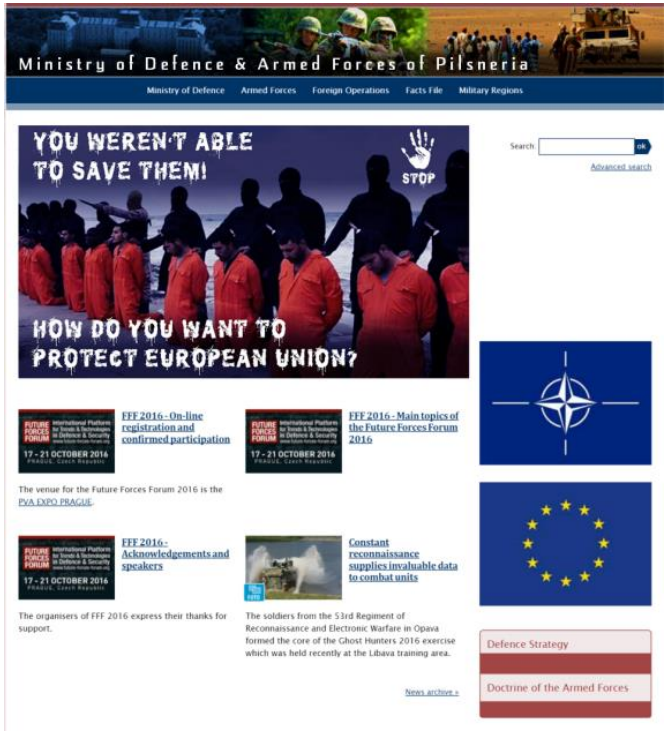
- Involvement of executives
- Reflecting a whole-of-nation response
- Implementing latest trends
- Emphasis on evaluation process
- Sharing best practices
- Incorporating different perspectives (private vs state…)
- Creating a non-threating and candid atmosphere



CZECH VIEW: WHAT IS GOOD

- Active involvement of professional journalists/press
- Consultations with subject-matter experts (academia, private, etc.)
- Incorporating in-house strategic analysis
- Not underestimating the value of a test run
- Making exercise eye-opening and impressive
- Graphic presentation is no less important





TAKEAWAYS AND OBSERVATIONS

- Decision makers hesitate to act
- Internal response plans have to reflect reality
- Media communication is essential
- Need for greater emphasis on cyber hygiene
- Use of exercise as a tool for measuring CIIP effectivity/efficiency

CONCLUSIONS

- Helping senior leadership to understand the importance of cyber for national security
- Testing real-world processes and incidents response plans
- All-inclusive approach – hyperconnectivity requires hypercollaboration
- Attractive scenario adapted for TA
- Continuous process including planning, execution and evaluation

TTX FOR HITCON PACIFIC 2018
–
INTRODUCTION

DISCLAIMER

Although some events depicted in this exercise are based on real incidents/occurrences, the exercise is fictitious and does not intend to link any nation/state/government/group of individuals to any wrongdoing in the real world. Nor does this exercise serve as an attribution tool. The links between nation states and other actors as well as events, locations, incidents and attribution hints are purely fictitious.

SCHEDULE

- Exercise will last **from 09:30 to 12:00** and will be followed by exercise debrief **from 13:20 to 14:00**
- Exercise debrief:
  - Will be prepared by organizers and presented in the afternoon (13:20 – 14:00)
  - Led by exercise organizers and facilitators.
  - Walks through the exercise and focuses on crucial aspects.
  - Aims to evaluate answers when possible. Does not always divide answers as being either correct or incorrect. It aims to identify crucial aspects, to compare answers, and to demonstrate, discuss and share different approaches, opinions and experience.
  - Aims to discuss the gaps in one's own structures and process found during the exercise by handling simulated crisis.

RULE NO. 1

DO NOT FIGHT THE SCENARIO, FIGHT THE PROBLEM

EXERCISE RULES (I)

- The exercise is not a test. There are no right or wrong answers.
- The purpose is to raise questions and to add friction into crisis management and the decision-making process.
- We expect that the participants, after completion of the exercise, will leave with more questions than answers.
- Decisions you make are not attributed to your organization or country.

EXERCISE RULES (II)

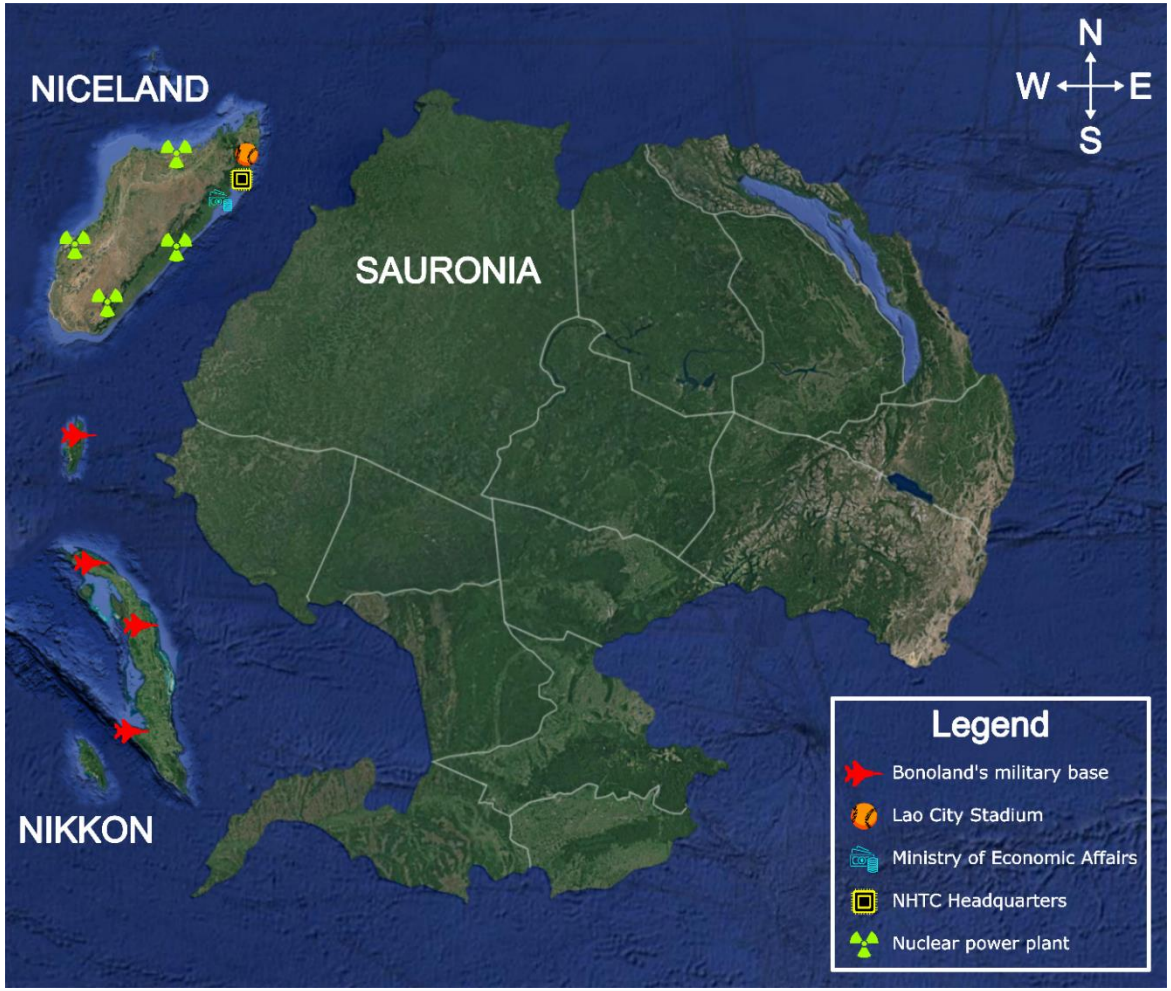
- Your background, whether it is technical, legal, or policy, does not play any role in the final outcome. What is important is your ability to deconstruct the process of making decisions and scrutinize the decisions undertaken during the exercise.
- The aim of the exercise is to illustrate how complex a solution to a cyber-related incident can be, and how many facets it has in all segments of governance.
- The views of intelligence, media, diplomacy, homeland security and defense should be considered before taking a decision.

EXERCISE RULES (III)

- The injects depict plausible cyber security events, based on real world examples.
- The scenario and all actors are purely fictitious.
- Without getting feedback from the participants, the exercise cannot be properly evaluated.
- **Exercise will be conducted in English but there will be a native Mandarin speaker to help participants at all times.**

REMINDER OF RULE NO. 1

THE STORY


NICELAND
SAURONIA
NIKKON
N
W
E
S
Legend
Bonoland's military base
Lao City Stadium
Ministry of Economic Affairs
NHTC Headquarters
Nuclear power plant

WHO PLAYS?

Countries:

- Niceland
- Sauronia
- Bonoland
- Nikkon

Non-state actors:

Niceland High-Tek Company a.k.a. NHTC

Sprinting Viper

NICELAND

- Home country of training audience (← that's YOU)
- Democracy
- Population of 30 million inhabitants
- Developed economy with manufacturing in information and communication technology (ICT) sector as a leading source of income
- Tourism is another source of income. More than 1/3 of inbound tourism originates in Sauronia, neighbouring country with which Niceland has complex and troubled relations
- Niceland's economy and even its citizens' way of life is highly dependent on modern information and communication technologies

ACTUAL FOOTAGE OF NICELAND'S PRESIDENTIAL PALACE

NICELAND

- Country has established national and government CERT teams, cyber security authority and legislation determining critical information infrastructure (CII)
- Niceland's offensive capabilities in cyber space are limited
- Niceland military established Cyber Security Command earlier this year as a semi-independent branch of the armed forces
- Niceland's sovereignty under threat from Sauronia

NICELAND'S FOREIGN MINISTER O'HELL von KITTY

SAURONIA

- Sauronia has more than 1.4 billion inhabitants
- Authoritarian regime
- Most citizens have access to internet but censorship of the content is among the most restrictive in the world
- Sauronia enjoyed high economic growth and currently possesses World's second largest economy
- Sauronia claims Niceland to be part of its territory

BONOLAND

- Bonoland is situated on different continent than Niceland and Sauronia
- It is a democracy with population more than 350 million people
- Bonoland possesses highly developed mixed economy including leading ICT companies
- Currently, it is a world superpower in military, political, and economic sense as well as a permanent member of the UN Security Council
- Bonoland maintains highly advanced offensive capabilities in cyberspace.
- Traditionally, it has close ties to Niceland
- Bonoland has strong economic relations with Sauronia, but the two countries consider each other strategic rival. Bonoland is militarily present in the region through its military bases in an allied country Nikkon

NICELAND HIGH-TEK COMPANY

- NHTC is the largest employer in Niceland
- It has several operations in both Sauronia and Bonoland
- NHTC is a recognized global brand and customers all around the world use NHTC's products
- Plans to introduce new generation of semiconductors
- NHTC is fifth largest manufacturer of smartphones (mainly NicePhone product line) and sixth largest manufacturer of notebook computers (NiceBook)
- Last year, NHTC won a contract to supply technology for Bonoland's major defense industry company Bonoland Defense Industries

SPRINTING VIPER APT

- Believed to be associated with Sauronia's civil intelligence service
- Cyber security companies, independent researchers, and state entities have linked multiple campaigns to this group
- Based on their modus operandi and tactics, techniques, and procedures they are apparently skilled and experienced group, operating in a stealthy manner
- They are almost exclusively involved in cyber espionage conducted against either state or private entities

WHO ARE YOU

- Participants are divided into multiple groups of 6 - 7 members. Each group represents a **Joint Task Force of Niceland** (JTF). Each group can only cooperate within the assigned group, not with other groups.
- As a body responsible for coordinating policy on national security issues, you are competent to make decisions **not** only in the field of cyber security.
- In formulating responses, **the JTFs are required to reflect the real national framework** they are familiar with from everyday life.

WHAT IS AT STAKE?

- 4 Main events
- Each of them represents major cyber security incident with real life implications
- All incidents were inspired by cyber attacks that happened in real world
- Failure to address the issues could have fatal consequences

WHO CAN PLAY?

- Everyone is welcome
- We especially encourage government employees, journalists and private sector technical experts
- Beauty of TTX is that everyone can learn something new:
  - Technical experts get insight into how real/life decision making looks like
  - Government employees learn something about complex challenges of cyber security incident
  - Journalists get experience that helps to communicate cyber security incidents to general public

DOS & DONTS

FORBIDDEN	REQUIRED	RECOMMENDED
Go back through events	Read Handbook and understand its content before STARTEX	Try to stick to dedicated time limit
Go forward through events	Discuss inside your group and try to reach a consensus	Not fighting the scenario, but fighting the problem
Discuss with other groups	Answer all questions	Use your devices to open and display exercise and audiovisual materials
Fill in multiple forms in one group	Write down if there is disagreement in your group	Ask NUKIB representatives to clarify misunderstandings
Create your own, new, geopolitical entities	Double check with Czech delegates before closing Google Form after ENDEX	Dedicate one group member to fill in the answers in Google Forms

Security Agency

OTÁZKY ODPOVĚDI 5

Main Event 5

Popis (nepovinný)

Inject 5.1

On May 2nd, multiple Estonian cities became a victim of a ransomware attack. Large cities as well as smaller municipalities have been among the victims. The total number of affected cities is around twenty. They have lost access to a large portion of their data which had been encrypted by the attackers. The attackers demand a ransom of 10 000 to 30 000 Euros in order to decrypt the victims' files. The attack has disrupted various services of municipalities, e.g. city workers' e-mail communication, on-line payments, local emergency services, court hearings, public transportation etc. Currently, there is no evidence to show that client or employee data has been compromised.

There have been other victims of the same type of ransomware, most of them in Estonia and several abroad. However, Estonian cities are the highest profile victims.

Název obrázku

IMPORTANT INFORMATION

EXERCISE

- **Runs from 9:30 to 12:00 in room R3**
- Register at the HITCON registration desk and receive ttx information package
- Bring your laptop

EVALUATION

- **Runs from 13:20 to 14:00 in R3**
- Observations from control team
- Real world inspiration
- Lessons learned
- Cookies…maybe…probably not though


COME TOMORROW
AND SAVE NICELAND
imgflip.com