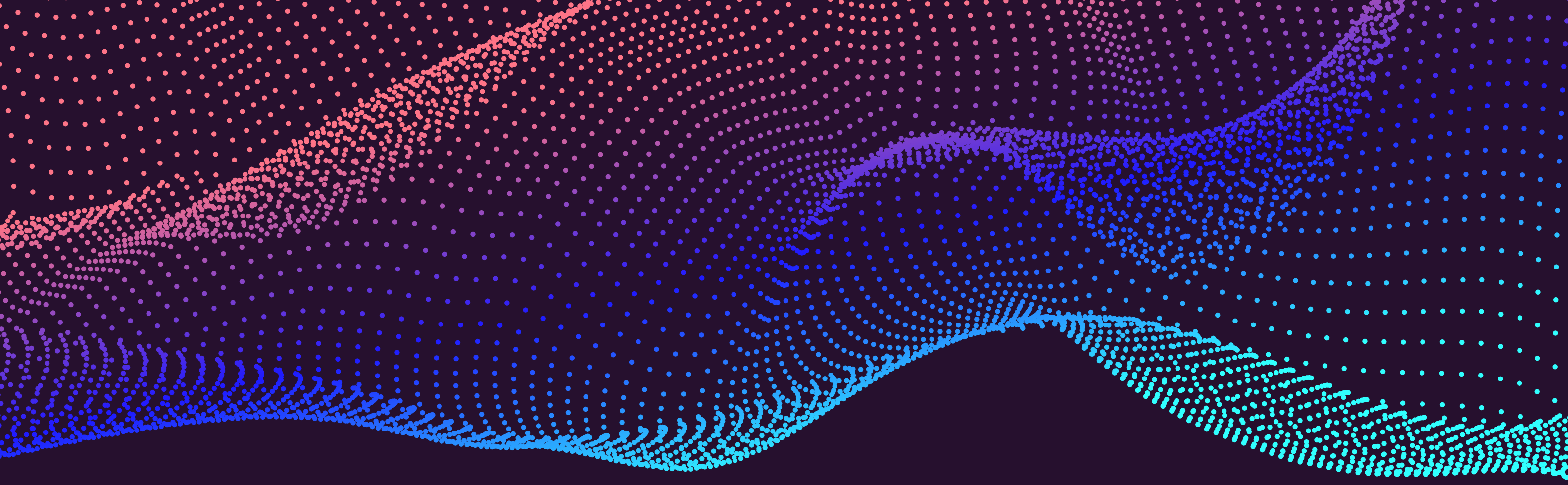
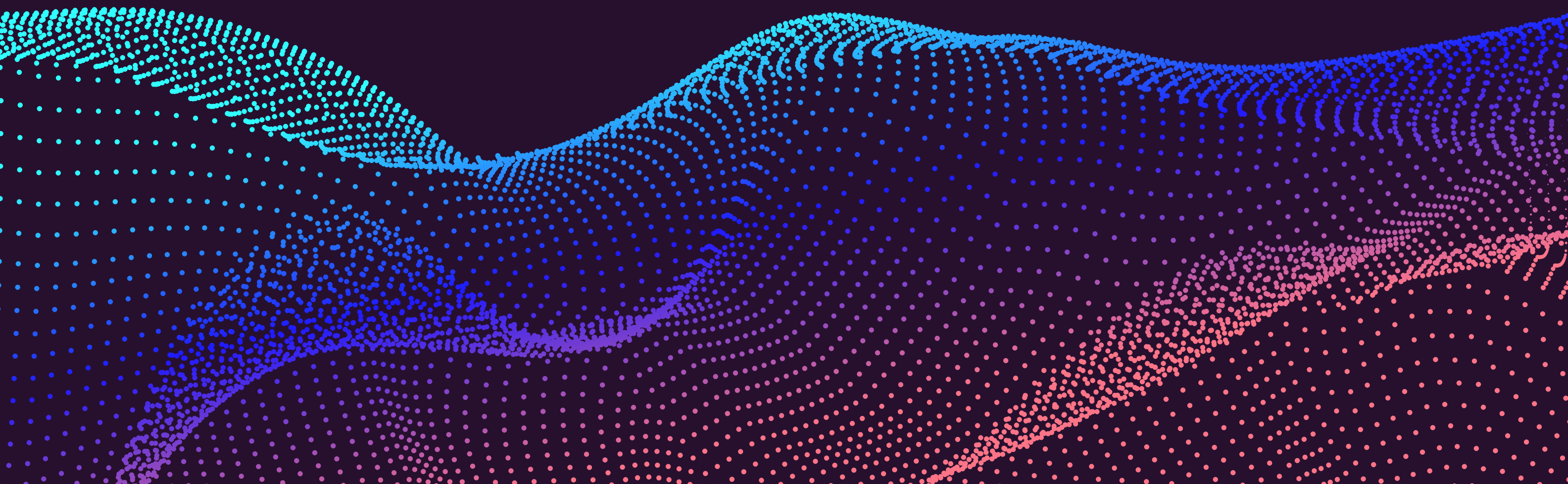


PERFECT SYMBIOSIS

CYBER SECURITY EXERCISES AND NATIONAL POLICIES

By **Veronika Netolická** and **Petr Novotný**, National Cyber and Information Security Agency of the Czech Republic



Cyber security exercises are perceived as one of the best tools for enhancing cyber security in the Czech Republic. They enable realistic crisis simulation in a controlled environment — and is there a better way to train/prepare for such a situation than to experience one? There are many useful and necessary tools (e.g., workshops, courses and conferences), but none can provide such a realistic opportunity as a cyber security exercise.

Like a Swiss Army knife, the exercises can be used for multiple purposes (see Figure 1). Such ability further underscores their effectiveness.

The ability to reveal and highlight blind spots in national policies can be achieved by various types of exercises — including technical, tabletops, procedural and communications exercises. Some are designed to check and assess national policies, while others might achieve that as a side effect.

Why assess policies by staging exercises? First, some policies may be obsolete. National policies and procedures might have been adopted long before critical systems became exposed to cyberspace. A good example is legal prescriptions for a state of emergency. These may have been in place for decades, but will they be of any use during a crisis in cyberspace? Second, assuming there is an up-to-date policy for active defense measures, how do you make sure it will be effective and applicable during an attack against critical infrastructure? It would surely be preferable to know before a crisis occurs. Finally, cyber security is a dynamic, quickly evolving field.

Policies need continuous updating, and the demand for new policies is ubiquitous. Consider the rollout of 5G networks: The next-generation of telecommunication networks represents a prime example of new technology that might create a need for novel national policies. Exercises have the ability to help reveal such demands.

When it comes to exercises, we apply a complex approach. Participants are invited from across all levels (strategic, operational and tactical), and all relevant aspects are covered (technical, political, economic, media, legal, ethical, etc.). Cyber security has been far more than a technical issue for the last couple of decades, spilling into other dimensions that include politics, the military, economics, legal issues and the media. These are all relevant to national policies. If these dimensions are covered in the exercise, appropriate participants must be present — legal experts, media experts, military officers and, especially, the decision-makers. In addition, it is a good idea to reflect new and upcoming trends in exercise scenarios. This helps to make them an effective tool in tackling emerging challenges.

Figure 1

MAPPING VARIOUS APPROACHES	IDENTIFYING BLIND SPOTS	REVISING POLICIES AND PROCESSES
IMPARTING KNOWLEDGE	PROVIDING INPUT ELSEWHERE	MAPPING THE STATE OF CYBER SECURITY
IDENTIFYING TRENDS	PROMOTING FOREIGN POLICY	SHARING EXPERIENCES

Source: National Cyber and Information Security Agency of the Czech Republic

Cyber security exercises are perceived as one of the best tools for enhancing cyber security in the Czech Republic. They enable realistic crisis simulation in a controlled environment – and is there a better way to train/prepare for such a situation than to experience one?

Synergy of exercises and national policies

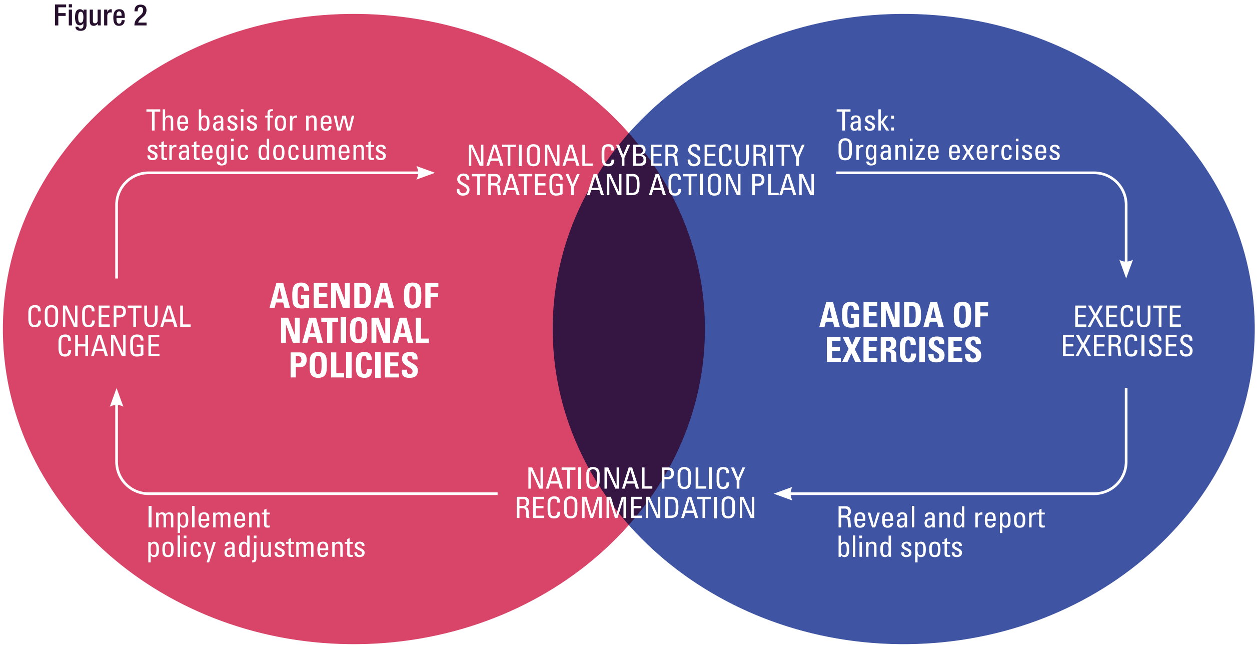
As shown above, revealing blind spots early is beneficial for drafting and adjusting effective national policies. Every exercise should aim to reflect the latest development with a focus on preparedness, which is closely related to a well-established and coordinated system. When a deficiency is detected, it is evaluated from the standpoint of the functionality of the national cyber security system. Based on the Czech experience, the process of identifying these spots in exercises is a closed circle of inputs and outputs. Inputs come from multiple sources — for example, previous exercises or their designers. However, the prime input contributors are national policy specialists. All of this input makes exercises sophisticated and more realistic. Output from the exercises should be relevant to national policy issues to be considered on an appropriate and strategic level. This process is based on people knowledgeable both in policy and in conducting exercises who can provide input suitable for the exercise and identify output fitting the purpose of national policy solutions.

The Czech experience and lessons learned

In 2016, the first document describing the blind spots in its national policies was introduced to the Czech government. The document was based on the Czech experience with the functioning of the system for ensuring national cyber security and contained analysis of the most fundamental problems that corresponded to the current framework. The outcomes of cyber security exercises are primary sources for this document. By processing these blind spots, it is possible to point out and focus on the primary lessons identified to make the process successful:

- **Workforce development** — People are a cornerstone of successful cooperation between the policy unit and exercise designers. Make sure they understand and appreciate each other's agendas and communicate regularly. The better input the policy unit can provide, the more valuable the outcomes will be. Allow national policy specialists to participate in or at least observe exercises, because if policy specialists understand

Figure 2


The basis for new strategic documents
NATIONAL CYBER SECURITY STRATEGY AND ACTION PLAN
Task: Organize exercises
CONCEPTUAL CHANGE
AGENDA OF NATIONAL POLICIES
AGENDA OF EXERCISES
EXECUTE EXERCISES
NATIONAL POLICY RECOMMENDATION
Implement policy adjustments
Reveal and report blind spots

Source: National Cyber and Information Security Agency of the Czech Republic

A nontechnical tabletop exercise is conducted at the Africa Endeavor Symposium in Ghana in 2019. U.S. AFRICA COMMAND

the aspects of cyberspace through participation in exercises and thus grasp the technical basics, they are better suited for creating policies. However, exercise designers can largely benefit when possessing knowledge of relevant policies on their own. Enable and support their education and self-development in areas other than exercises. Such an approach will pay significant dividends in the future.

- **Selection** — The selection of deficiencies to be identified as blind spots must be commensurate with the nature of national policies and must be prioritized. When the system is not fully developed, prioritization is critical.
- **Whole-of-government approach** — A national cyber security system includes many stakeholders (e.g., critical national infrastructure operators, regulators, internet service providers and law enforcement). In this respect, relevant organizations should be included to address and negotiate over the blind spots. Cyber security at the national level cannot be ensured solely by one dedicated institution. The side effect of this process is to establish trust, which has been essential in the case of the Czech Republic.
- **Consistency** — Ideally, a document addressing the blind spots should be produced regularly since exercises frequently reveal blind spots as well. Presenting such a document annually is frequent enough and sustainable.
- **Offering a solution** — The product should not only draw attention to revealed insufficiencies in the system. It is essential to present solutions based on previous discussions with the relevant entities. Such an approach is significant for subsequent implementation. Unsurprisingly, exercises can be relevant in this process as well. When the blind spot is encountered during an exercise, participants often try to come up with a solution. Sometimes international participants share best practices from their countries. This might represent another precious outcome of the exercise to be included in a blind spots paper.
- **Continuous evaluation** — The evaluation process should work retrospectively and provide honest feedback on the effectiveness of previously applied solutions. The effectiveness of new policies might be a good topic for a new exercise.
- **Keep the circle running** — The ecosystem of identification and sharing the input and output should be never-ending, comprehensive and dynamic because insufficient information sharing or evaluation could generate a new blind spot. □