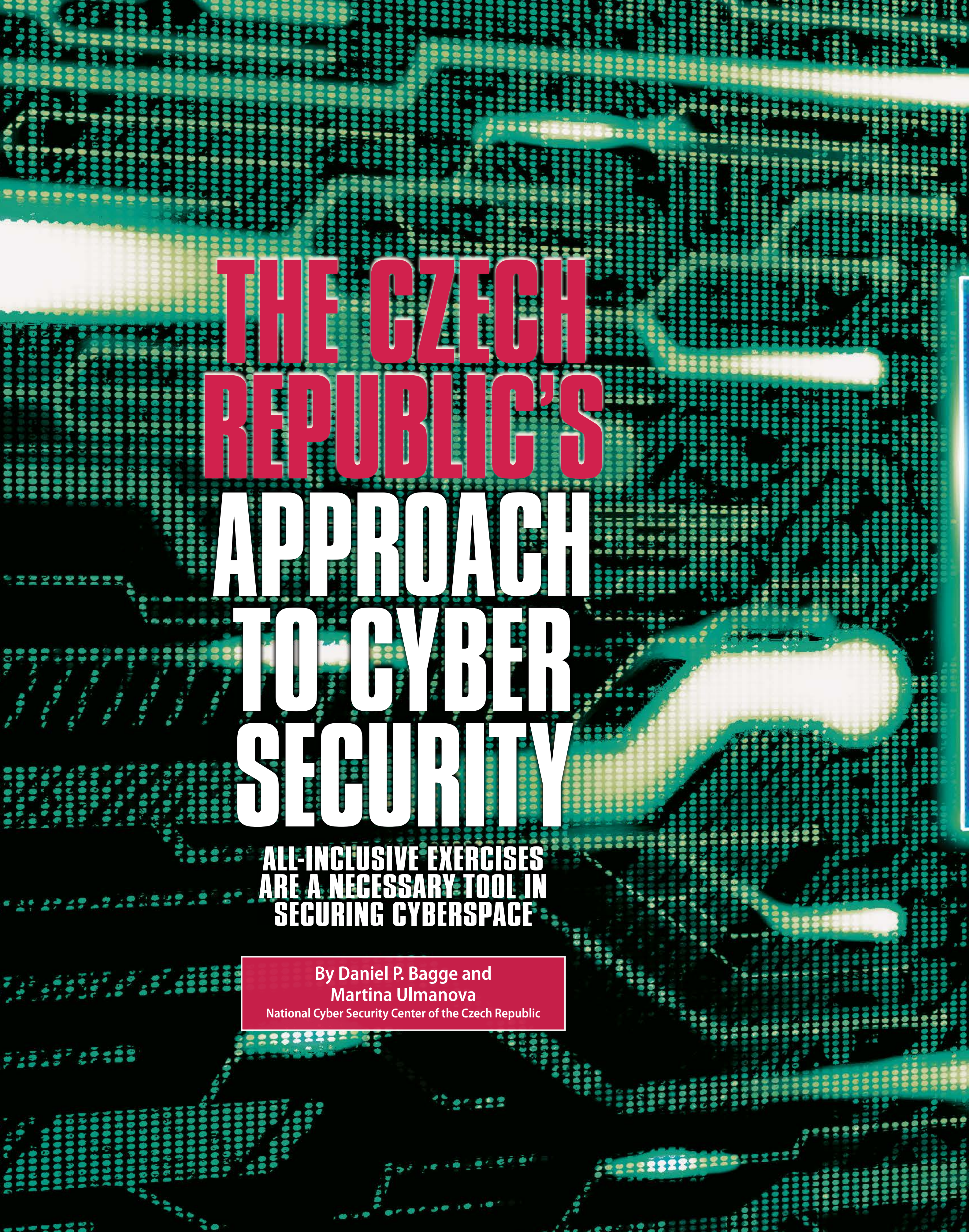
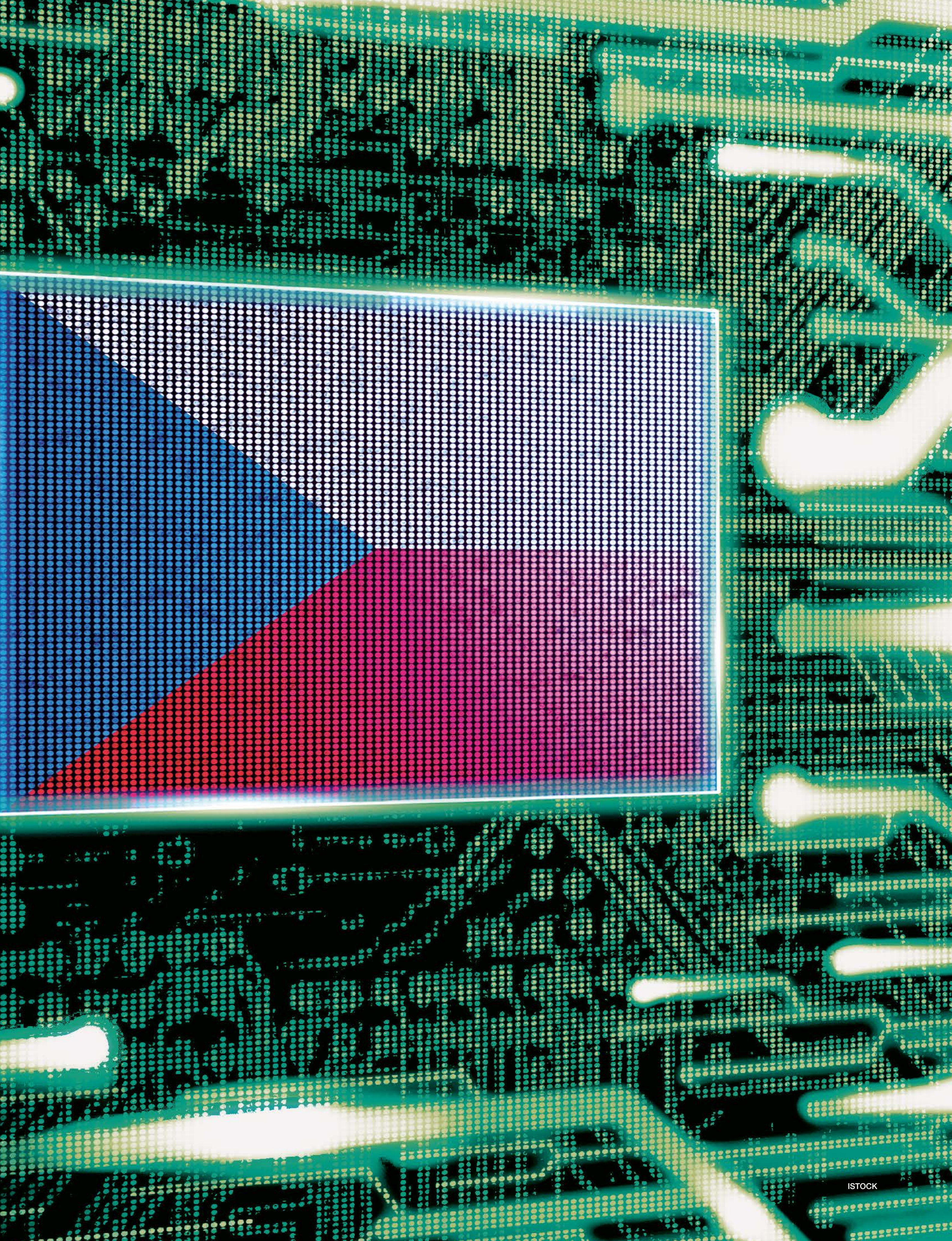


THE CZECH REPUBLIC'S APPROACH TO CYBER SECURITY

ALL-INCLUSIVE EXERCISES ARE A NECESSARY TOOL IN SECURING CYBERSPACE

By Daniel P. Bagge and Martina Ulmanova
National Cyber Security Center of the Czech Republic



ISTOCK

The rapid pace of technological innovation makes it difficult for those who aren't immersed in the cyber security field to fully understand the threats posed by cyber-savvy terrorists and criminals. This is especially true for governments and private institutions that are mostly unaware of the potential impacts when these technological innovations are turned against them. The new methods and sophistication of attacks and the expanding number of targets are frequent topics of public reports and debates. A society exposed to this kind of information expects its government to be prepared by creating a resilient and secure cyberspace. But how can a government stay ahead of evolving technology, particularly when bureaucratic systems tend to be slow in responding to challenges that are mostly unknown to the decision-makers?

Consequently, staying up to date on technology developments, and being able to quickly adapt to new threats, requires being cyber-knowledgeable. However, information technology (IT) experts and those employed in the technology industry cannot be fully aware of the implications that IT products and solutions have on national security. Technical personnel on operational levels and cyber security managers are not familiar with the processes of political, diplomatic and strategic decision-making. They often live in the narrow tech world. Likewise, senior leadership, law enforcement officials and policymakers face difficult challenges in their work without knowing the technological implications and impacts associated with cyber incidents.

Getting technically skilled professionals to understand the governmental challenges, while at the same time getting government representatives to deepen their understanding of the possible impacts of cyber-related incidents, presents a real challenge. Because of limited time and a lack of tools on a national level to educate people on a large scale and in a timely manner, the best way to address this challenge is through cyber security exercises.

Not only do they have a direct impact on the skill set of participants, they can provide a real-time evaluation of lessons learned. Cyber security exercises can be divided into a few types: tabletops, technical, hybrid or procedural, with slight overlaps among them. All types enable participants to tackle the important aspects of responding to incidents, such as teamwork, information sharing and institutional cooperation.

While technical exercises can be easily imagined by our general audience — a group of IT professionals and Computer Emergency Response Teams battling over each other's infrastructure and defending perimeters through keyboards and screens — decision-makers on a higher level cannot solve the complexities of a cyber crisis by hitting a keyboard button. Senior leaders do not face cyber-related challenges on a daily basis and may not be capable of adequately assessing the crisis and giving the right orders to lower echelons. Therefore, exercises aimed at decision-making processes are a unique opportunity for exposing senior leaders to relevant cyber-security matters. This, combined with realistic scenarios, is the best way to educate senior leadership on the importance of cyber security and its relevance to national security. One might argue that having the technical capacity might be sufficient to solve a cyber security incident or crisis, but that is not true. Although technical/operational cyber experts possess the skills and best technologies, without the relevant command and control, there is no use for them.

Moreover, there is another trend that we must be aware of in this digital age. Alongside the knowledge gap between technical staff and decision-makers, we must deal with varying capabilities and skills between younger and older generations. While young people have been widely exposed to an increasingly open Internet and find it easily accessible, the Internet age was unimaginable to many senior executives when they started their careers.

THE CZECH EXPERIENCE AND PRACTICES

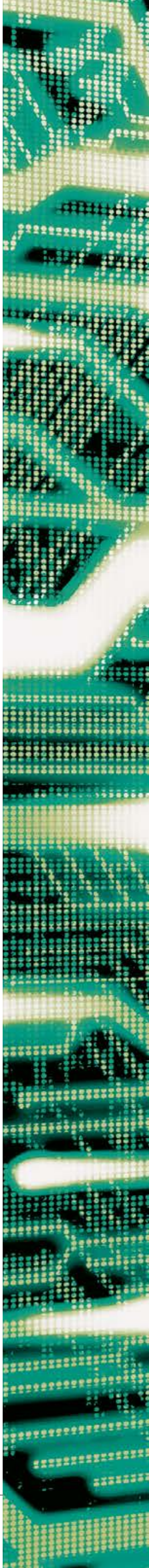
In the Czech Republic, we understand the need to continually train in both the technical skills and the communication and procedural aspects of cyber security. Therefore, the National Cyber Security Center (NCSC) participates regularly in exercises on an international level, including the Crisis Management Exercise and Cyber Coalition, both organized by NATO; the Locked Shields exercise organized by the Cooperative Cyber Defense Centre of Excellence; and Cyber

> IN THE CZECH REPUBLIC, WE UNDERSTAND THE NEED TO CONTINUALLY TRAIN IN BOTH THE TECHNICAL SKILLS AND THE COMMUNICATION AND PROCEDURAL ASPECTS OF CYBER SECURITY.

Europe, organized by the European Union Agency for Network and Information Security. Apart from participation in these international exercises, NCSC organized and participated in two national exercises in 2015: one tabletop designed for strategic leaders and decision-makers and a technical exercise for information and communications technology (ICT) administrators and specialists.

The Strategic Decision Making Exercise and Exercise on Cyber Crisis Management held in Prague in June 2015 was a joint initiative of the Czech National Security Authority, the European Cyber Security Initiative (Estonia) and the European Defense Agency. The exercise examined the state's ability to make decisions and efficiently use available resources to counter a cyber crisis. During the three-day event, nearly 40 participants, representing national government, military, intelligence services, the private sector, police, prosecutors and other law enforcement agencies, faced an escalating and very realistic scenario. The scenario was divided into six phases and continuous storylines with various forms of cyber threats presented. Each working group had different sets of information, requiring members to cooperate effectively. The results, including a graphic visualization of the exercise, were closely analyzed and a follow-up event was held with the main stakeholders and participants. The aim of the exercise was not to name a winner, but to identify gaps and shortcomings in decision-making and verify communication channels during a crisis based on real-world scenarios that escalated from minor incidents to military involvement and a state of emergency.

In September 2015, the NCSC was tasked with developing and carrying out a tailor-made tabletop exercise based on a real-world threat actor for the Department of Defense and U.S. Cyber Command in Washington, D.C. The exercise covered cyber/information warfare, cyber espionage campaigns, electoral propaganda, leakage of sensitive information, and code versus content hacking, among other topics. The exercise sought to raise awareness of the political and national security implications associated with significant cyber incidents and highlight the complexities of a decision-making process. The event was evaluated by participants



as a success and will be repeated in 2016. The tailor-made tabletop exercise was updated in early 2016 and conducted in June at the NATO ACT, Norfolk. The exercise was also conducted within the Visegrad 4 Cyber Security Workshop, organized by the presiding Czech Republic, in Washington D.C. The Czech Republic is willing and has the capacity to share its expertise in conducting tailor-made cyber security exercises at the strategic level. At the end of 2015, the NCSC carried out a special tabletop exercise for students in the master's program for security and strategic studies at Masaryk University in Brno.

Participants at the international cyber defense exercise Locked Shields 2016 HANS-TOOMAS SAAREST, ESTONIAN DEFENCE FORCES

TECHNICAL EXERCISES

The first national technical cyber security exercise, Cyber Czech 2015, was conducted last year. It was organized by the National Security Authority, which is the overarching body of the NCSC, in collaboration with the Institute of Computer Science (ICS) at Masaryk University. It took place in a special, virtualized training environment called the Cyber Proving Ground (KYPO) at ICS. The opposing forces squared off in this unique, sealed-off computer system, where any code or solution can be tested without risk to external networks. The exercise was designed to expose participants to real-world cyber attacks. The scenario placed teams into a fictional rapid-reaction force of the Czech Republic. The teams were asked to assist a nuclear power plant where the ICT and ICS systems had been under massive attack. Although the defending teams were competing, the exercise encouraged information sharing and cooperation.

It was the first technical exercise in which participants from key governmental entities and other relevant authorities of the Czech Republic could participate alongside each other. Subsequently, another iteration of the exercise was conducted in March 2016. Private entities of critical information infrastructure, operating particularly in the energy sector, were given the same opportunity to participate. To underline the importance of such exercises, the prime minister of the Czech Republic personally attended the exercise. The exercises were novel in their magnitude and for allowing participants and observers to gain experience defending a significant piece of critical infrastructure. Cyber Czech was the first test of the scenario, which is also meant for use for academic research as well as by public institutions and private companies. Not only did the teams respond to attacks and technical problems, they also assessed potential legal and media impacts. Those two aspects — legal and media — are included in all national exercises because they are considered integral parts of solving potential crises and necessary to ensure cyber security.

To date, two kinds of exercises have been presented. However, based on the experience gained during these events, the NCSC realized that there is time for a hybrid approach. That means connecting the technical exercises with strategic level tabletops along with conventional crisis procedures to ensure that all national security entities are prepared for a large-scale crisis. This involves crisis management entities, the intelligence community, national security bodies, and stakeholders from the military, academia and the private sector.

FURTHER DEVELOPMENT OF EXERCISES

Exercises in the past were divided mainly in two domains — technical and tabletop. However, these domains are intertwined with the complexities and tools necessary to solve the problem set. It is

insufficient to train only technical or top-level leadership through specific exercises based on their lines of work. In a cyber crisis, they will have to coordinate responses and actions and share information not only horizontally, but also vertically. Exercises where these two worlds cooperate must be encouraged. Additionally, the private sector, academia and the media must be involved. The media is a relevant stakeholder, possessing a key to solving cyber crises. They play a crucial role in not only informing the public during cyber security events, but also in forming general public opinion. This is important in light of the rising importance of strategic communications and the overall resilience of society in understanding information operations campaigns. Last but not least, the media have a significant role in the aftermath of cyber crises. Events are often assessed not by the way they were technically handled, but how it was handled publicly. Therefore, the NCSC is planning a series of workshops for journalists to acquaint them with the techniques and importance of strategic communications and how to recognize information warfare techniques. Media representatives are regularly invited to participate or observe the exercises. The private sector often holds information vital to the solution, but governmental bodies still do not appreciate their position at the table.

Apart from conducting hybrid exercises on a national level, the future of cyber security also lies in greater international cooperation and exercises involving diverse technical and cultural backgrounds. This can be done through enhanced international cooperation between states, academia and the private sector. In the Czech Republic, we have the aforementioned KYPO, which is of academic origin based on security research and collaboration with the National Security Authority. Another cyber exercise arena is the privately owned Cyber Gym, the European branch of the Israeli Cyber Gym Co. Connecting these two cyber exercise ranges with similar installations around the world will greatly enhance the ability to train with teams that, despite the universal language of information and communications technology, have different cultural approaches to problem solving, as well as capabilities aimed at different threats.

Interconnecting private, governmental and academic entities in a global cyber security exercise might not be a new concept; however, incorporating the technical part, the tabletop and spanning continents with cyber arenas is indeed new. It could simulate, in the best possible way, future conflicts between state and nonstate actors.

Widening the scope of the exercises and including scenarios that follow recent events are useful, but that's not enough anymore. Exercises using past incidents as a model are great for enhancing the situational awareness of participants. However, to best utilize the advantages of a cyber security exercise, it is crucial to forecast and prepare for the unexpected. Therefore, the NCSC is creating a fluid structure within the exercise-planning working group called the red cell. It is designed to enhance forecasting of possible trends and incidents and to design events that are unlikely within regular planning structures. Another issue of great concern is incorporating intelligence services into technical exercises. Therefore, the NCSC facilitates remote participation from its facilities to respect the nature of their clients' covert activities.

CONCLUSION

If policymakers understand the aspects of cyberspace through participation in exercises and thus grasp the technical basics, they are better suited for making policy. Through cyber security exercises, the gap between the policy world and technical world is narrowed and the outcomes of policy planning are tied to technical possibilities.

Getting top leadership involved in decision-making during exercises results in better decisions during crises. With a deeper appreciation gained during mockups, they do not perceive cyber as strictly IT stuff and something utterly impossible to comprehend. In preparing complex exercises, the NCSC strives to incorporate all levels of the "food chain" from the operational level to the tactical level and to the strategic level.