October 2022 · Equal Authorship Julia Schuetze & Rebecca Beigel

Cybersecurity Policy Exercises in Practice

Learnings from Implementing Tabletop Exercises in Different Countries

Stiftung
Neue
Verantwortung

Think Tank at the Intersection of Technology and Society

Executive Summary

Citizens as well as public and private organizations are exposed to tremendous risks by the constantly evolving cyber threat landscape. This development is being tackled by governments all over the world through the implementation of cybersecurity policies and regulations, among other means. Designing cybersecurity policies, however, is a complex challenge that requires specific skills and interdisciplinary contributions. One tool that can be used to contribute to this endeavor, to bring stakeholders from different backgrounds together and discuss and test policies, is cybersecurity policy exercises.

From July 2021 to July 2022, we designed and implemented cybersecurity policy exercises in eight countries from different parts of the world, including the Republic of Armenia, the Republic of Costa Rica, the Republic of Kenya, the United Mexican States, and the Republic of South Africa. The exercises, except for the one in Costa Rica, were part of a joint project with the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), which was implemented on behalf of the BMZ. Some of these exercises took place on-site, whereas others were carried out online because of the COVID-19 pandemic. They typically convened participants from governmental and private sector institutions, civil society organizations, and academia. Before the implementation, we studied the theoretical foundations of how cybersecurity exercises can be used for policy work[1]. We then identified the exercise type that best fit the context we worked in—that is, cyber capacity building—and developed a methodology and a process for designing and implementing exercises with stakeholders from different countries.

We experienced firsthand that cybersecurity policy exercises are useful tools, for example, with which to practice information sharing and analysis across sectors during an incident. This utility stems from the fact that such exercises offer participants the opportunity to discuss a hypothetical yet realistic cyber incident scenario and to experience policy responses. However, a crucial learning from our work is that to unfold the benefits of these exercises and ensure that they have a lasting effect, a number of points must be considered during design and implementation. In this paper, we outline our most important learnings and present several

[1] Beigel & Schuetze (2021) “Cybersecurity Exercises for Policy Work - Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work”, Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/de/publikation/cybersecurity-exercises-policy-work

practical suggestions that might be helpful for other workshop designers and facilitators. For greater clarity, we structured our experiences into four categories: organizing, designing, implementing, and evaluating an exercise.

Country-specific cybersecurity policy exercises demand extensive methodological insights and detailed knowledge of a country's cybersecurity policy. We therefore recommend conducting research and expert interviews on a given cybersecurity architecture, legislation, and policy. Additionally, we have come to the conviction that exercises in the context of capacity building are sustainable and correspond with objective realization only when supported by and co-organized with local (political) stakeholders. Such support can come in the form of pre-workshops, wherein the overall objectives of an exercise are discussed, or expert interviews that focus on country-specific questions, such as the particular responsibilities of national cybersecurity stakeholders. Both these preparatory processes influence how a scenario is formulated.

During cybersecurity policy exercises, participants not only practice their national incident response but also examine what real-life impact cybersecurity policies have during an incident. An exercise that focuses on policy helps shed light on processes that are in place. It also enables participants to experience a lack thereof when policies have not been translated into clear processes, such as incident reporting. Participants may additionally address other concrete objectives, such as to increase awareness of the existence or non-existence of cybersecurity policies or the practice of information sharing between different sectors.

Aside from applying these practical learnings on designing and implementing cybersecurity policy exercises, we recommend that cybersecurity policy exercises, particularly those conducted as part of cyber capacity building initiatives, be regarded not merely as a means of practicing national incident response in a one-off manner. Rather, they should be seen as a chance to identify gaps and missing pieces in existing policy processes. They also offer the opportunity to create multi-stakeholder dialogue afterwards and collect concrete ideas and formats to work on challenges identified in the exercise. Moreover, we found considerable interest among stakeholders from different countries in implementing additional exercises to monitor developments over time. We hope that our learnings advance the work of implementers, enable those interested in the field to take their first steps, and, ultimately, facilitate exchange on the methodology.

Table of Contents

Introduction

Twenty men and women wearing business attire gather at a U-shaped table. They all have at least one thing in common—they work on cybersecurity policy in the same country. Someone from the national Computer Security Incident Response Team (CSIRT) is nodding to a colleague who works at the ministry responsible for crafting the IT security law. A diplomat from the foreign office approaches us, asking for an agenda, while the chief information security officer from a critical infrastructure provider is getting coffee. A female representative who works for an organization that aims to increase the number of women in cybersecurity unpacks her laptop.

The composition of the group, and which institutions and organizations are represented, depends on the country in which the exercise takes place. Some of the participants have not met before. They are here to have a shared learning experience. In our introduction to the exercise day, we emphasize that there are no right or wrong answers. We point out that our exercise is an opportunity to immerse ourselves in the process and learn from it—and from each other. Then, the cybersecurity policy exercise starts.

Between July 2021 and July 2022, we[1] designed and facilitated eight cybersecurity policy exercises in countries in different regions: the Republic of Rwanda, the Republic of Kenya, the Hashemite Kingdom of Jordan, the Republic of Costa Rica, the United Mexican States, the Republic of South Africa, the Republic of Kosovo[2], and the Republic of Armenia. The exercises, except for the one in Costa Rica, were part of a joint project with the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), which was implemented on behalf of the BMZ. Some of the exercises—like the one from which we took the exemplary scene above—took place on-site, others online.[3] There is a wide range of cybersecurity exercise types that can be used for policy work. We described their respective features and benefits in our previous paper that explores the theoretical foundations and the potential of cybersecurity exercises in the context of policy work.[4] The kind of exercise that we chose to implement and that we refer to in

[1] Apart from the authors, the team consisted of the the Stiftung Neue Verantwortung's (SNV) director for international cybersecurity policy, a student assistant and cybersecurity advisors from Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH.

[2] This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence. This statement is congruent with the position of the European Union.

[3] Originally, when the project started, all cybersecurity policy exercises were meant to be held in person. However, the COVID-19 pandemic demanded a (temporary) change to a virtual environment.

[4] Beigel & Schuetze (2021) "Cybersecurity Exercises for Policy Work - Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work", Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/de/publikation/cybersecurity-exercises-policy-work

this paper is the so-called tabletop exercise. Tabletops usually entail a hypothetical yet realistic cyber incident scenario. Participants talk or play through the scenario, assuming fictional roles or the positions they have in real life, depending on the design of the exercise.

Our exercises took place in the context of cybersecurity capacity-building. In our theory paper, we stated that one instrument that enables decision-makers to create better policies is cybersecurity exercises[5]. This is because rather than just reading and memorizing information about real-life circumstances, participants of such exercises can actively learn about and even experiment with processes and policies[6]. To tell what a policy really means and determine how it works, cybersecurity exercise tasks can, for example, shed light on the processes and decisions taken when the policy is implemented[7]. In our eight tabletops, the tasks and discussions focused on the impact that policies have on the national response to a cyber incident.

Cyber capacity-building demands that a range of stakeholders work together across borders, implement and coordinate projects together and share cybersecurity experiences[8]. For cyber capacity-building work, in particular, cybersecurity policy exercises are thus an effective method for contributing to building trust in multi-stakeholder environments, developing bridges between policy content and its practical implementation and providing a “platform” for the local cybersecurity community to exchange ideas in a safe environment.

The exercises in this particular project aimed to address one or more of the following objectives previously identified by the project team and prioritized by national cybersecurity policy experts from the respective countries that participated in the tabletop exercises that followed:

- Increase education/awareness of cybersecurity
- Practice sharing of information and analysis by different institutions

[5] Beigel & Schuetze (2021) “Cybersecurity Exercises for Policy Work - Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work”, Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/de/publikation/cybersecurity-exercises-policy-work

[6] Beigel & Schuetze (2021) “Cybersecurity Exercises for Policy Work - Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work”, Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/de/publikation/cybersecurity-exercises-policy-work
Dewar (2018), “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf

[7] Beigel & Schuetze (2021) “Cybersecurity Exercises for Policy Work - Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work”, Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/de/publikation/cybersecurity-exercises-policy-work

[8] Collett & Barmpaliou (2021), "International Cyber Capacity Building: Global Trends And Scenarios", European Union Institute for Security Studies, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf

- Practice public communication measures
- Increase understanding of legal requirements and implemented policies
- Improve collaboration measures between sectors (national level)
- Identify cooperation measures between national and international stakeholders
- Practice assessment and analysis of incidents
- Clarifying the responsibilities of institutions
- Increase cyber resilience more broadly, for example, through business continuity and processes in place.

Generally, some exercises are designed as competitions in which participants are evaluated on whether they manage a cyber incident scenario in the intended manner. In other formats, exercises can be used for maturity assessments in which evaluations play a major role in determining how advanced a response is. However, our objective was different. In this particular case, it was essential that we emphasized that we, as exercise implementers, were not interested in judging or evaluating, for example, national policies or even individual decisions made in the exercise with specific criteria in mind. This was particularly important for us, as we were working in countries other than our own. Our role was to provide a safe environment for participants to practice and draw on their own lessons learned through this experience.

After holding eight exercises in eight countries, on-site and online, we can conclude that cybersecurity policy exercises are a useful and important tool for preparing national stakeholders to respond together to cyber threats. However, in order for these exercises to be implemented well and to have a sustainable effect, a number of points must be considered. It is crucial to be familiar with the social, political and legal contexts and with the cybersecurity policies and architecture of the exercise country, as all of these conditions affect the exercise design. Moreover, we found that ideally, the exercise is organized with the support of a local expert or partner organization to ensure that the exercise has the necessary impact and takes all the relevant stakeholders and their needs into account.

Now that we have gained broad experience implementing cybersecurity policy exercises, we would like to share these and other insights with the growing community of people interested in designing and implementing such exercises. In this paper, you will find our learnings from a year of cybersecurity exercises, structured in four main categories (organizing, designing, implementing and evaluating). This categorization, as well as the consecutive numbering of our learnings , is intended to help individuals look up specific information when they are planning, creating and implementing exercises.

Learnings

Organizing an exercise

1. Choose between virtual or on-site exercises

Due to the Covid-19 pandemic and related restrictions, we had to find alternatives to on-site exercises; thus, we developed a virtual exercise format. Looking back, we had good experiences with virtual settings, particularly given the benefits of more flexible participation, reduction in our carbon footprint and cost savings (mainly the costs of flights and the venue). These benefits may be considered when planning an exercise in the future.

When planning a virtual exercise, certain requirements have been proven helpful to consider. In our experience, it is useful to connect stakeholders beforehand to build trust, for example, with pre-exercise activities, such as bilateral meetings. In addition, we recommend checking participants' internet connections beforehand or identifying a place near most participants where they can go for a stable internet connection. This is to avoid disruption or frustration caused by internet issues or dropouts. Limiting the duration of the exercise to approximately 3.5 hours can reduce the probability of people being distracted by their daily work activities. It is also essential to allow for short breaks to avoid virtual fatigue.

From our experience conducting in-person exercises, we can say that such an on-site format is particularly beneficial when there is high commitment by a local partner organization with a local network, and the exercise is run with the intention of kick-starting a long-term initiative that may include follow-up measures, such as workshops, awareness materials or network meetings. Moreover, if one of the goals is to create a community or increase trust among stakeholders who have not met before, an on-site exercise is much more suitable for getting to know each other and creating a safe environment for sensitive discussions. In-person events can also be longer to accommodate not just the exercise but also other, more informal formats, to create networking opportunities.

2. Map tasks and skills

A wide array of tasks must be completed to implement a cybersecurity policy exercise, ranging from organizational (like event management) and technical tasks (such as working with digital tools) to moderating and writing duties (e.g., drafting the scenario on which the exercise is based). Preparing an exercise also requires different skills and knowledge, for example, in IT security, cybersecurity policy and legislation, international relations and international cooperation, or storytelling. For organizations new to this method, it may help to map out the different skills needed and tasks implemented across the four main categories: organizing, designing, implementing and evaluating. In the table below, we have created an overview of tasks and skills that we needed when organizing, designing, implementing and evaluating a cybersecurity policy exercise. It may be useful to distribute tasks among different people or organizations.

Overview of tasks and skills for cybersecurity policy exercise implementation

	Organizing	Designing	Implementing	Evaluating
Tasks	• Liaising with funders/clients (if applicable) • Organizing a pre-workshop • Engaging with various stakeholders, e.g., participants or (local) cooperation partners • Building local networks • Increasing awareness of the exercise format and process • Managing budgets • Keeping track of tasks • Sending out a pre-survey and a feedback survey	• Researching country policies, laws and cybersecurity architecture • Identifying open questions for the pre-workshop • Identifying the objectives of the exercise • Designing the pre-workshop • Writing role sheets • Writing the scenario, e.g., attack types, and technical details • Drafting exercise components (e.g., tasks according to exercise objectives) • Writing role sheets • Writing the script, including timing • Identifying questions for reflection	• Testing the technical/logistical set-up • Drafting the agenda • Moderating the pre-workshop • Moderating the exercise • Moderating the reflection	• Writing a summary of the reflection • Identifying possible follow-up measures • Analyzing submitted tasks • Providing feedback • Engaging with participants on follow-up measures and analyzing potential improvement points
Skills	• Stakeholder management • International relations • Event management • Cultural understanding	• Storytelling • Knowledge of cybersecurity (policy) • Knowledge of IT security • Writing • Method expertise • Research • Digital tools	• Public speaking • Moderation/Mediation • Organization • Knowledge of participants/group dynamics • Knowledge of scenario design	• Analysis • Evaluation • Knowledge of cybersecurity (policy) • Writing • Cultural understanding
	Support staff for local/regional, logistical and technical expertise			

3. Coordinate tasks between stakeholders

Of course, it is possible for one person to take on tasks in different categories. In addition, people at different organizations can cover tasks across various categories. However, we have noticed that coordination can be a challenge when tasks are covered by different organizations. When not all of the tasks above are performed within one organization , a checklist of tasks can help coordinate and cooperate across organizations and people involved. Moreover, it is important to be aware of how certain decisions made by organizers can impact others' tasks, such as exercise designers. For instance, a question that designers faced before every exercise was: Is it essential to draft a whole new scenario, or is it possible to use an existing scenario and make country-specific context adaptations to the exercise components (information, decision, tasks and meeting)? Discussions about this decision had to consider the resources available and the expectations of the stakeholders, such as funders or participants. Organizers usually do this, but in this case, the designers' knowledge was equally important, such as country-specific research and understanding the impact of objectives on tasks. For such reasons, a joint kick-off meeting and even regular Jour Fixe meetings are highly recommended to maintain an overview across people and organizations. Another method we used took inspiration from software development, the so-called the so-called SCRUM methodology[9]. SCRUM is a framework[10] for developing and sustaining complex products. It allows for frequent iterations and continuous feedback during project management and helps to make sure that the delivered end product, the exercise, suits the stakeholders' needs. As we organized more than one such exercise and relied on a diverse number of stakeholders for implementation (in- and outside our own organization) and therefore were operating within a dynamic work environment, we used the SCRUM framework. As a team, we kept track of tasks to flexibly adapt to changes. This proved useful, for example, during the Covid-19 pandemic, when plans changed quickly due to travel restrictions and adaptations from on-site events to virtual formats.

[9] "The term scrum is borrowed from rugby, where it is a formation of players. The term scrum was chosen by the paper's authors because it implies teamwork. The software development term scrum was first used in a 1986 paper titled „The New New Product Development Game" by Hirotaka Takeuchi and Ikujiro Nonaka."
"Scrum", In Wikipedia, Accessed 28/9/2022, from https://en.wikipedia.org/wiki/Scrum_(software_development)

[10] Agile Scrum Belgium, "What's so Great About Scrum Methodology?", Accessed 28/9/2022 https://www.agile-scrum.be/whats-great-scrum-methodology/

4. Have local experts as co-organizers

Throughout the project, we found that it is crucial not only to engage with local stakeholders during our country-specific research or the pre-workshop but also to cooperate directly with a local cybersecurity expert of the partner country. Ideally, the exercise is co-organized with a local partner organization. Local experts or local partner organizations may, for example, contribute country-specific cybersecurity knowledge, engage with potential participants, build partnerships and organize logistical and technical support, which is crucial for an in-person exercise. In addition, we found that input by a local cybersecurity expert for all participants before the exercise is a good start to the exercise day. Certain information, for example, current government ideas on new institutions or laws, may still be in development. In those cases, a policy input that focuses on the current situation helped create relevance and ownership from the start.

Designing an exercise

5. Invest in detailed country-specific research

A country's policies and positions on cybersecurity issues often depend on its social, historical and cultural environment. Familiarizing ourselves with this environment helped us lay the groundwork for the exercise design, which had to be realistic. It also prepared us for collaboration with stakeholders from different countries. Moreover, some exercise participants also identified the exercise objective of learning about laws and policies. In most countries, a systematic and accessible overview of the respective cybersecurity policies (legislation or architecture) was missing. Therefore, early in the project, we decided to make our research publicly available and published so-called Country Profiles[11]. This research included open-source desk research and was supported by discussions with local experts. These profiles included information on the political system and the socio-political background to provide an overview of country-specific particularities, the respective cybersecurity policy, information about a country's threat landscapes, the legal framework and key documents shaping the cybersecurity landscape, important (government) actors in this field and information about multilateral cooperation.

[11] Stiftung Neue Verantwortung, „Cybersecurity Policy Exercises“, Accessed 28/09/2022, https://www.stiftung-nv.de/en/publication/cybersecurity-policy-exercises

6. Hold a pre-workshop to determine the objectives

Each exercise is highly dependent on the specific exercise objective(s)[12], which should be determined before the exercise with stakeholders from the respective countries. To validate the exercise objectives and better understand the exercise environment, we recommend implementing a (virtual) pre-workshop with stakeholders knowledgeable about the topic and environment who will later participate in the exercise. Ideally, the composition of participants should include diverse perspectives, for example, from different disciplines and sectors.

In our experience, it proved useful to include a workshop session to discuss and prioritize the potential exercise objectives (e.g., to practice communication after an incident or to train specific aspects of incident response, such as information sharing). This gives workshop participants the opportunity to articulate why they think a certain objective should be addressed with the exercise. Additionally, participants may discuss the responsibilities and responses of their institutions. This discussion helps to verify whether stakeholders relevant to the national response are already participating and whether certain tasks match what participants would do in real life (e.g., writing a press statement). In addition to the discussions, which were primarily useful for us as exercise designers and implementers, the workshop allowed future participants to network and build trust with people they did not know before.

7. Identify participants

To guarantee having relevant stakeholders at the table, we started selecting the exercise participants early in the process. Which institutions and individuals are important stakeholders in cybersecurity (policy) and, for example, incident response? Which disciplines should be covered by the group of participants? Who is the target audience (young professionals or decision-makers at the highest level)? In our context, it was particularly beneficial to include stakeholders from all different sectors—the government, the private sector and civil society—to have people from all sectors experience the effects of national cybersecurity policies in place. We also included other professional groups, such as journalists, when the exercise emphasized public communication and the media. For another exercise in which the incident focused on mobile payments, it was important to include payment providers from the private sector in particular.

[12] Beigel & Schuetze (2021), „Cybersecurity Exercises for Policy Work - Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work", Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/de/publikation/cybersecurity-exercises-policy-work

We mapped the expertise and responsibilities beforehand, with the help of the partner's knowledge. If publicly available, documents on the cybersecurity architecture[13] were a starting point for identifying important stakeholders. In addition, the pre-workshop was a way to engage with potential participants and identify missing ones. Bear in mind, however, that this process takes time—regarding not only the identification and selection of participants but also trust-building and engaging participants to prevent dropouts later. Throughout the entire process, we were mindful of diversity and inclusion and thus, for example included organizations focused on women's rights. We also reflected continuously on the dynamics between institutions and even individuals to be mindful about their political, cultural or historic relationships—for example, the relationships between government agencies and civil society organizations.

8. Write the scenario first

The exercise design was more efficient when we first wrote down the whole scenario instead of starting with other elements, such as tasks . The scenario is the backbone of the exercise. For us, it is an approximately three-page-long story, including technical information about the incident, information on the threat actor, the political environment and the domestic laws that are directly connected to the incident and the ensuing response. We tend to include information that may later be used to write exercise components , for example, Information such as media articles (Information) or Tasks. At this stage, it is also important to identify which will be made public to which stakeholder group during the exercise. Some information about the scenario may not be shared with participants at all, but it is essential to design a coherent exercise. An example is to write about the threat actor and its motivation for conducting cyber operations. This may never be revealed to the participants of the exercise, but it is crucial to possibly give them hints for the analysis of the incident. Having this storyline beforehand helped us envision potential questions that could come up before we drafted exercise components such as tasks.

[13] Herpig & Rupp (2022), „ Germany's Cybersecurity Architecture", Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/en/publication/germanys-cybersecurity-architecture

9. Think in terms of exercise components

For a successful exercise, we recommend thinking about different elements, which we call exercise components.

Information means information about the initial scenario that the participants receive, as well as the developments of that initial scenario. All of this information can be provided in different ways, for example, via a fictional CSIRT, an intelligence briefing provided by fictional technical experts, a fictional Secret Service employee or the media that is part of the exercise. Participants can influence the way the exercise plays out with Decisions, which are different courses of action the participants can take. For example, a decision on whether or not they would investigate an incident would, of course, lead to more or less access to information. Their decision to share a certain piece of information with another group could impact the cooperation between these groups.

The heart of the exercise is Tasks, which, in this case, focus on cybersecurity policy and processes. As our focus was on policy, it was crucial to include tasks that help to reflect on the policy implementation or development, such as tasks regarding what an initial notification process looks like or assessing the national security impact. In addition, response tasks—such as writing a press release—were particularly important to us in a cybersecurity policy exercise to make the participants experience the impact of policy. Finally, we provided opportunities to meet across groups. These Meetings are useful for stakeholder groups, as they provide an opportunity to eliminate misunderstandings or enable joint responses like a joint communication that was not even foreseen in the policy but made sense in the moment.

10. Design templates but adapt if needed

When creating exercises, it is helpful to think about efficient ways to design exercises and save materials that have worked well and could be re-used or adapted. Our learning is that templates, such as Tasks or Information, can help design the exercise because we did not have to start from scratch each time. Instead, we can focus on adapting the task to a new context. Whether this is possible, however, depends on the decision that comes before creating the components of exercises. Before every exercise, we faced the question of whether we needed to draft a whole new scenario for the planned exercise or whether it was possible to make adaptations to the existing scenario and the exercise components fit, in our case, a country-specific context and fulfill the objectives of the exercise. When writing a whole new scenario, all underlying technical details potentially need to be changed. This is sometimes necessary if the objective is very specific. In one case, the exercise was supposed to help identify responses when a certain mobile payment system was affected. In another case, an international company through its supply chain was supposed to be affected. Then, to create an exercise that fits the context, it might be necessary to write a whole new scenario, including the attack types - even if this is more costly in terms of time and labor than adapting an existing one.

To make this decision, we used country-specific research , a pre-survey and a pre-workshop to identify which underlying scenario would best fulfill the objectives. When we found that the existing scenarios did not work, which happened in two cases, we decided to draft new ones.

This assessment is why building templates for the Information component of the exercise is not always useful. For example, drafting audio of a CSIRT representative that includes technical details depends a lot on the country and the incident context; therefore, re-using details can lead to copy-paste errors. Thus, it is better to get inspired by other exercise information components, but do not simply copy and paste them.

However, some exercises have a more general objective of testing a national policy on cooperating with the critical infrastructure that is being developed. In this case, the designers may need to adapt the Information component of the exercise to the country-specific context: What critical infrastructure is affected, and how many people? However, the underlying attack type can be more general, such as ransomware.

Moreover, adapting templates helps us understand exactly where specific policies take effect . For example, is sharing the incident report voluntary or mandatory? Is there a specific format that the country uses to report on an incident, such as an existing report template?

In one exercise, the focus was on considering refugees' ability to use payment services despite a cyber incident. In the response task, in which we created a template, we decided to include questions to address this topic specifically. For example, we asked the government what non-governmental organizations (NGOs) it would cooperate with to provide money to refugees during an outage. This aspect came to our attention after we talked with local human rights NGOs, which brought up that they would usually be the providers of emergency cash. It was important to add this question because it increased the awareness to include not just staff that focuses on fiscal policy and cybersecurity but also staff from international relations, communications and human rights. In the reflection, the observation was made that it is advisable to include stakeholders from outside the government in the cyber incident response, such as human rights organizations.

Therefore, templates can serve as a starting point for exercise designers. However, it is crucial to be open to developing new tasks and adapting templates according to the country-specific context and objectives to be addressed.

11. Provide realistic interaction possibilities

We chose to include possibilities to interact between groups (the component called Meetings) in the exercise design, for example, by including opportunities to share information via email, or in person. However, to keep it realistic, we did not organize the meeting up front. This is important because, in some cases, improving cooperation across sectors or practicing the sharing of information was among the exercise objectives. To give a realistic account of what the status quo behavior would be, we chose to offer the opportunity to meet but did not set up meetings without the participants' initiation. Thus, if a group did not want to meet other stakeholders, the group experienced the consequences of this decision. We then could reflect on this component afterward in the reflection session, where participants identified challenges, observations and follow-up measures together.

12. Focus on concrete policy features

In order to tell what a policy really means and determine how it works, or whether it has the effect it aims to have, the component Tasks on the processes and decisions made when the policy is implemented. One such task is "Describe the initial notification process in your country," a task that seems simple but can reveal whether legal requirements are fulfilled and in what way. The private sector and the government can experience directly what effects incident reporting has. In addition, the task might raise practical process questions: Who should be informed, and how to get in touch? By encrypted website submission or by phone?

No exercises are the same because countries' policies are not the same. In some countries, reporting is mandatory; in others, it is not. One country requires critical infrastructure to report incidents; in another country, this applies only to certain sectors. Some request reports within 24 hours and others within 75 hours. In one country, the law even defines that if it is a level-red rated incident (the most severe incident impact), the entity affected by the incident must report within 24 hours and then every eight hours after that. In this country specifically, the task asking to assess the incidents' severity had to be distributed at the same time as the "notification process" task, given the interconnectedness of the processes. In this case, the exercise tasks revealed that, at the very beginning of an incident, without any time to gather enough data points, it may be very hard for participants to provide an accurate assessment of the severity—possibly leading to too little contact across sectors after the initial incident assessment.

In our experience, it is useful to create tasks that focus on specific policy features. This helps participants experience the impact of a law or policy in a fictional yet realistic environment. The playful manner creates an open discussion environment that helps participants reflect on the law together. We have also seen non-tangible improvements that are important for effective cybersecurity management, such as an increase in trust and understanding among participants from different sectors who had never met before or were skeptical about each other. Some comments made during the reflection session illustrated this point: "We are friends," and "We have so much more in common than we thought."

13. Use authentic visualization but do not overdo it

When designing materials for an exercise, we faced the choice between a more realistic or a more abstract look while also considering our budget, skills and time. We decided that the more likely it is that participants would encounter a similar situation in real life, the more accurate and authentic the material should be. This was supposed to help the participants feel that the exercise was real. At the same time, it was important to remind participants of the exercise environment by using playful corporate design/branding because we wanted to create an open learning environment and avoid a testing or competitive appearance. For example, if the exercise included a ransomware message, it would help participants immerse themselves in the exercise if the message *looked* authentic, mimicking the real user interface and language, which we recreated with graphic design software. However, we felt that we should not send a real message to participants' phones as this would invade their privacy, and be more of a gimmick. When recreating a press conference, for example, we also aimed for a very realistic representation of the situation. We created pressure by letting professional journalists ask questions about the planned response, which then helped participants prepare for the actual response to a cyber incident. Designing the exercise is a balancing act between keeping it real and using design in a way that supports a safe and learning environment.

14. Prepare participants for the exercise

To determine common ground in an often heterogeneous pool of stakeholders and even more importantly, to bring participants into the right "exercise mindset," it is essential to prepare them thoroughly. Exercises are highly engaging and interactive environments, demanding a lot of input from participants and the willingness to immerse themselves in a specific role and its responsibilities. Sometimes, this might be difficult, as participants might have had a stressful week at their offices and difficulty adapting to play through a scenario that may happen or being open to unknown tasks. The importance of preparing participants for this experience and providing them with the necessary information during preparation should not be underestimated. Despite this preparation, however, it is important to go through all these materials again on the day of the exercise to recall all the important information.

Information to provide to the participants in advance may include logistical information of the exercise (e.g., where and when to meet or access information to the call, if implemented virtually), the preliminary agenda and participant lists. It is particularly essential to forward material to participants that helps them get used to and identify with the exercise environment and the roles they are supposed to play. These materials may include character and/or role sheets or even information on the initial exercise scenario. In our case, the role sheet outlines which stakeholder group (e.g., the private sector) a participant represents in the exercise. Role sheets are one means of outlining what responsibilities the group has (e.g., to advise a bank affected by an incident on how to respond "to the incident"), what kind of resources and expertise they have access to and to highlight the environment the group is operating in during the exercise. The role sheet may also indicate how the group relates to other stakeholder groups (e.g., public–private cooperation). The participants' roles can, but do not have to, reflect their real-life professions.

Implementing an exercise

15. Write a script for smooth implementation

Implementing a cybersecurity policy exercise is complex because the initial cyber incident scenario develops continuously, and the different participant groups need to receive the different exercise components at the right time. For example, groups need new information at the right moment to be able to work on an incident assessment. Participants also need to be provided with information that triggers decision-making as well as tasks to solve. The timing for distributing information, decisions and tasks is very important to guarantee a smooth exercise performance and is crucial to address the objectives. For instance, participants can practice sharing information only if they have received the necessary information. Due to the number of participants or participant groups and the complexity of the exercise, several implementers often work together and need to coordinate.

We have determined that a script helps give an overview of the different actions that implementers need to take as well as of the timing. The script can be adapted to the needs of the implementers and the context, but may, for example, contain the following information: phases of the exercise (such as the assessment phase, response phase etc.) with timings (e.g., the assessment phase takes 25 minutes). The script may then outline which information or task is given to the respective stakeholder groups at what time. If different stakeholder groups are involved in the exercise, the script should include information about each respective group of the exercise, or a separate script should be prepared for each group. This should also include information about how one group's decisions may impact another group. The script may also help determine when and how to include breaks in the exercise without accidentally getting participants out of the "exercise mindset" and focus.

Although a script can be of great help in preparing and implementing an exercise, flexibility is still required for a successful exercise. Be prepared to deviate from the script when it is necessary to react to unforeseen circumstances. For example, a group may decide to work on tasks or questions that are not part of the prepared material. In such cases, it is inevitable to spontaneously adapt the prepared material, information flows and/or schedule accordingly.

16. Practice before implementing the exercise

Due to the exercise's previously mentioned complexity, it is useful to practice it among implementers. Even while the script is being written, especially after it has been completed, several practice runs are worthwhile. The run-throughs involve all implementers. It is particularly important to pay attention to timing (e.g., handing out the exercise documents, such as decisions or tasks), preparing for interaction among groups (when group A potentially shares information with group B), and anticipating potential challenges (where might there be challenges in the process, and how might problems be mitigated?). Practice runs provide an opportunity to think through very practical questions: "How do implementers communicate with each other when they are in different (virtual) spaces?" or "How do implementers deal with groups completing the exercise at very different speeds?" Make this a priority to guarantee smooth implementation.

Evaluating an exercise

17. Evaluate without judging

We work with professionals from different countries, many of whom are in expert and high-level positions in the field of cybersecurity. Telling them how to do it "the right way" would seem somewhat presumptuous, so we chose not to assess the outcome from our outsider perspective. For ownership purposes, we decided that most of the evaluation should be done by the participants among themselves, especially in this multi-stakeholder environment. We provided only the method and space to do it. With the reflection session, we allowed participants to share their observations, criticism and ideas for possible follow-up formats. Later, we summarized the results in written format and shared them among the participants. If there was interest in examples engaging with other countries, we offered inspiration for how to set up an exchange on, for example, best practices. We analyzed the submitted tasks without an assessment sheet. Instead, we focused on highlighting whether the groups had differing views on a subject matter and what impact this had on the response to an incident. We also provided all the materials to participants after the exercise so that they could do the same.

Sometimes, this was a challenge for us. In one exercise, we had a team of journalists involved in order to practice public communication. This team first interviewed the affected financial provider who quite openly shared information about the incident, shared mitigation measures and gave advice to customers. However, when the journalists moved to the government group to interview them, too (which the government group had agreed to beforehand), the government denied that there was even an incident—a difficult situation for all, as it created distrust between the stakeholder groups and did not align with our values. Afterward, we confirmed with them that this was not due to lack of information but was their preferred public communication strategy. This resonated with previous government practices in the country. In this case, we raised awareness of the impact of the action and shared ideas for possible steps to create trust after the exercise. We also followed up with the journalists to inquire whether this was a cyber-specific issue; they later explained that it was not. Although this was a difficult moment for us as implementers of the exercise, we stuck to our approach of not judging. Learning about how other exercise implementers would have reacted in this situation would be interesting for us.

18. Follow up after the exercise

When wrapping up the exercise day, it proved useful to communicate clear follow-up steps to the participants. These steps may include sharing with participants the materials developed during the exercise. It is also advisable to take notes on lessons learned from the course of the exercise and the subsequent reflection, abstract them afterward and share them with the participants. This allows people to come back to the documented points and derive and implement follow-up actions, if necessary.

It proved useful to provide contact details for follow-up questions or feedback. It can also be helpful to prepare a feedback survey that includes broader questions about the exercise set-up and methodology, as well as more specific questions, for example, on how the exercise helped improve the understanding of certain cybersecurity policies or response measures or which objectives were particularly well covered in the exercise. This survey can then, for example, be used to improve the exercise methodology or to plan follow-up measures. In addition, when sent over time for multiple exercises, a survey allows for comparability of specific aspects or questions. Follow-up communication with the participants should follow in a timely manner after the exercise.

Outlook

From our experience using cybersecurity policy exercises in international cyber capacity-building, they can be an effective method for contributing to building trust in multi-stakeholder environments, developing bridges between policy content and its practical implementation, and identifying potential follow-up measures to be implemented within the local or regional cybersecurity community. We moreover found that to achieve the intended objectives, as outlined in the Introduction, for example, to raise awareness of cybersecurity policies, a full-scale exercise design and implementation must consider several aspects while organizing, designing, implementing and evaluating an exercise.

When organizing an exercise, make sure to map the tasks—from organizational tasks (such as event management) to creative tasks (such as writing the scenario)—that are necessary to implement the exercise successfully. In addition, make sure to have knowledge of the project team's skills to distribute responsibilities accordingly. Throughout the process of preparing the exercise, make sure to be dynamic and implement iterative processes—for example, through regular Jour Fixe meetings and the SCRUM methodology. Finally, make sure to collaborate with local cybersecurity experts with country-specific knowledge and networks.

When designing an exercise, we recommend investing resources in country-specific policy research and holding a pre-workshop that allows for the definition of exercise objectives by local cybersecurity experts who will later be exercise participants. This is a crucial step in adapting the exercise to country-specific needs. Furthermore, it may simplify the design process if the full scenario is written at the very beginning of the design process and other exercise components such as information, tasks and decision questions are then built afterward.

For the successful implementation of an exercise, ample preparation is very important. In our experience, it is worthwhile writing a implementer script with information about when and how to interact with the exercise groups to structure the complex process of an exercise implementation. Just as important as creating the script is practicing it ahead of time and running through it with all the exercise implementers.

When evaluating an exercise, make sure to give ownership to the participants. Offer a platform to reflect on challenges and lessons learned from the exercise, rather than to assess the outcomes as an external party. Make sure to document the reflection and share it with the participants afterward. This enables local institutions to further engage with the contents, share them with colleagues or use them as a basis for follow-up activities.

Overall, we found that the exercises used in the context of capacity-building should not necessarily be the means to an end. This was confirmed by exercise participants who shared their desire to continue to work on the subject matter and who identified follow-up measures that emerged from the exercise. In the reflection sessions following the scenario-based work of the exercise, participants identified ideas to improve cybersecurity in their country, among others the development of written guidelines or online training on best practices for incident response communication; the development of policy incentives for incident reporting and the identification of what civilian-focused cybersecurity means in their respective countries.

Thus, we believe that stakeholders who implement cybersecurity policy exercises in the context of capacity-building should consider them not only as a means of practicing national incident response but also as a way to identify gaps, offer the opportunity to create multi-stakeholder dialogue afterwards and identify concrete ideas and formats to work on challenges identified in the exercise in the future. Moreover, we found that there was great interest in holding additional exercises to monitor developments over time, engage with fellow participants further or include additional stakeholders.

Finally, as part of the project, we reflected on the resource-intensiveness of exercises and are interested in engaging with others to explore ideas on how exercises can be made more accessible to potential exercise implementers who lack, for example, financial or personal resources. Feel free to get in touch with us to discuss this further. We hope this paper is only a starting point for engaging with others who are new to designing and implementing exercises or who have experience in exercises themselves and would like to exchange views on the topic .

Acknowledgments

The exercises, except for the one in Costa Rica, were part of a joint project with the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), which was implemented on behalf of the BMZ. We would like to thank - in no particular order - all cybersecurity policy exercise and pre-workshop participants, co-organizers, speakers, the Trust4Cyber Team from GIZ, and the BMZ.

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent, non-profit think tank working at the intersection of technology and society. The core method of SNV is collaborative policy development, involving experts from government, tech companies, civil society and academia to test and develop analyses with the aim of generating ideas on how governments can positively shape the technological transformation. To guarantee the independence of its work, the organization has adopted a concept of mixed funding sources that include foundations, public funds and corporate donations.

About the Authors

Julia Schuetze is project director for International Cybersecurity Policy at the Stiftung Neue Verantwortung e.V where she manages multiple projects. Her research focus is on comparative cybersecurity policy, European cybersecurity policy, cyber operations against election processes and cyber resilience of local government entities. She also designs and implements multi-stakeholder cybersecurity policy exercises in different countries.

Rebecca Beigel is a project manager for International Cybersecurity Policy at the Stiftung Neue Verantwortung e.V.. Her work focuses on German cybersecurity policy and on cyber capacity building. She also designs and implements multi-stakeholder cybersecurity policy exercises in different countries.

Contact the Authors:

Julia Schuetze
Project Director for International Cybersecurity Policy
jschuetze@stiftung-nv.de
+49 (0)30 81 45 03 78 82

Rebecca Beigel
Project Manager for International Cybersecurity Policy
rbeigel@stiftung-nv.de
+49 (0)30 40 36 76 98 3

Imprint

Stiftung Neue Verantwortung e.V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97
https://www.stiftung-nv.de/en
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Alina Siebert