April 2021 · Rebecca Beigel & Julia Schuetze

Cybersecurity Exercises for Policy Work

Exploring the Potential of Cybersecurity Exercises as an Instrument for Cybersecurity Policy Work

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Table of Contents

Executive Summary

Malicious cyber activities are increasing worldwide and getting increasingly more sophisticated. Individuals, businesses, and governments explore different ways of tackling this development, for example, through developing policies to counter or mitigate cyber threats. One promising instrument for doing so is cybersecurity exercises. Different cybersecurity exercises (e.g., red team/blue team exercises, cyber wargames, workshops, tabletop exercises, and simulations) can address different audiences and goals – from examining technical responses by critical infrastructure providers to assessing diplomatic responses to a cyber incident. To grasp the potential of cybersecurity exercises – particularly for policy work – it is important to explore the different types of exercises in more detail.

The paper first highlights defining features of each cybersecurity exercise type to emphasize each type's advantages. Workshops, for example, are speculative, collaborative, and can improve understanding between different actors. Meanwhile, simulations can replicate reality as much as possible using digital networks, which helps simulate attacks and the reactions to such attacks. Secondly, the different exercise types are applied to different stages of the policy cycle – a cycle mapping policy work from defining a problem to the implementation and evaluation of a policy - to explore reasons for using them at certain stages of policy work. Simulations, for example, are particularly beneficial to use when implementing or evaluating a policy, for example, for testing its effectiveness.

The paper creates a simple guide for exploring the potential application of cybersecurity exercises for policy work and for strategically using them. It is recommended to go through a three-step process to find whether cybersecurity exercises are an instrument to be used for a specific policy objective.

1) Firstly, scope out the policy work – consider the policy work at hand and the target audience to be reached.

2) Secondly, identify the stage of use – identify where the policy work is best situated on the policy cycle.

3) Thirdly, consider the defining features of cybersecurity exercise types and identify which exercise type is the best to achieve the policy work goal.

Ultimately, the paper highlights that cybersecurity exercises are an instrument that decision-makers should consider when developing cybersecurity policies and/or aiming to achieve different cybersecurity policy goals.

Acknowledgments

This paper was supported by experts through an online collaboration and a joint virtual workshop. The views and opinions expressed are solely those of the author and do not necessarily reflect the opinions of the experts or the respective employers. In alphabetical order, acknowledging essential contributions of:

We would like to thank

Enrico Calandro, Cybersecurity Capacity Centre for Southern Africa, University of Cape Town

Robert S. Dewar, Geneva Centre for Security Policy

Sarah Theresa Fischer, Deutsche Gesellschaft für Internationale Zusammenarbeit

Sven Herpig, Stiftung Neue Verantwortung

Neil Jenkins, Cyber Threat Alliance

Maurice Haesen Kajangwe, The Ministry of Information Communication Technology and Innovation (MINICT) Rwanda

Franz Lantenhammer, NATO Cooperative Cyber Defence Centre of Excellence

Sönke Marahrens, German Institute for Defense and Strategic Studies

Divya Ramjee, American University

Tomslin Samme-Nlar, Gefona Digital Foundation

Nick Small, EU Cyber4Dev

Nailah Ukaidi, Smart Africa

Edrine Wanyama, Collaboration on International ICT Policy in East and Southern Africa

The study is part of a project about country-specific cybersecurity exercises financed by the Federal Ministry for Economic Cooperation and Development (BMZ), commissioned by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

Introduction

Malicious cyber activities[1] are increasing worldwide and getting increasingly more sophisticated.[2] This development presents a challenge to individuals, businesses, and governments, resulting in the need for cooperation between stakeholders to mitigate these threats, respond to them, and become more resilient.[3] To counter such cyber threats, decision-makers aim to find instruments to enhance the cyber threats' prevention, detection and the reaction and response to them to mitigate the impact of malicious activities and respond effectively.[4] Over the years, stakeholders have, therefore, implemented different instruments to do this and to achieve various complementary goals in their cybersecurity policies and strategies.[5] One instrument that enables decision-makers to create better cybersecurity policies is exercises.[6]

Different types of cybersecurity exercises are defined in the literature.[7] This paper explores these five cybersecurity exercise types: cyber wargames, red team/blue team exercises, workshops, tabletop exercises, and simulations. Although most of these exercises are also used in other policy fields, such as workshops or tabletop exercises, this paper focuses on cybersecurity and using these exercises for cybersecurity.

Implementing cybersecurity exercises can serve different purposes. It can, for example, help decision-makers enhance their understanding of cyber threats, challenges, and opportunities or create more effective cyber responses by ensuring information sharing and collaboration among many different actors. Cybersecurity exercises could help improve skills for handling cyber incidents on technical, legal, or policy levels.[8] Also, cybersecurity exercises can be used to achieve specific policy purposes – for example, an increased understanding of cybersecurity-related matters and policies – and as a means to make policy, for example, drafting or evaluating policies.

Therefore, cybersecurity exercises are used by a range of stakeholders that include governments, the private sector, civil society, and universities or think tanks, among others.[9] The exercises are usually beneficial for creating or testing policy to accelerate policy understanding or for leadership to better understand their role in a national response plan. Crucially, cybersecurity exercises enhance participants' knowledge of the functioning of and interrelation between digital infrastructures, legal frameworks, and policy requirements.

Despite the potential benefits of cybersecurity exercises, several challenges come with using them. Practitioners are not automatically familiar with exercises as an instrument for cybersecurity and vice versa; exercise experts might be unaware of cybersecurity-related topics.[10] Hence, it might be difficult for decision-makers, such as policymakers, to understand the various potential applications of cybersecurity policy exercises. In addition, many different types of exercises can address multiple

purposes and contexts. Cybersecurity exercises are used for policy, technical, legal, communication, or even educational purposes – sometimes simultaneously.

It is, however, necessary to have a better understanding of cybersecurity exercises to fully grasp the potential use cases for policy work – not just to reach policy objectives but also enhance policy development processes. This paper examines cybersecurity exercises as an instrument for policy work. First, it sets out the different types of cybersecurity exercises and explores their respective features. This approach enables a better understanding of their advantages, particularly for policy work. Second, the paper discusses cybersecurity exercises along the policy cycle to guide decision-makers regarding when and how to utilize exercises effectively. A more precise understanding of the cybersecurity exercise types, their differentiation, and their use, particularly for policy work, could add to making cybersecurity exercises more recognized as an instrument to be implemented in the policy context and achieve the desired policy outcomes.

1. The Potential and Challenges of Cybersecurity Exercises

As instruments of training, exercises have a long tradition that dates back beyond antiquity. They became a teaching method at business schools in the 1950s and spread into qualitative fields like policy in the 1990s.[11] Exercises offer an active learning experience independent of their intended purpose and use. Cybersecurity also benefits from such an active and experiential learning tool. Cybersecurity exercises give participants the opportunity "to use skills, techniques, tools and policy frameworks"[12] in a practical environment rather than "simply memorizing information."[13] This active learning experience contributes to a better understanding of real-life circumstances.[14]

The literature defines different types of cybersecurity exercises.[15] This paper focuses on cyber wargames, red team/blue team exercises, workshops, tabletop exercises, and simulations. Most of the exercises discussed here, such as workshops or tabletop exercises, can be or are also being used in other policy fields. In this paper, they are discussed solely in the context of cybersecurity, and are described as "cybersecurity exercises" as others have done before.[16]

These cybersecurity exercise types can work with (hypothetical) scenarios that might or might not include a policy dimension. Scenarios are a foresight[17] method of telling stories about possible future conditions and the path toward them.[18] Cybersecurity exercises can use technical infrastructure and a "virtual or secured digital network"[19] (such as simulations), or they can use a discussion-based format, such as in the case of tabletop exercises. Discussion-based exercises can be run virtually through digital platforms and instruments, which is particularly important during the COVID-19 pandemic. It is also possible to use more technical exercises, such as red team/blue team exercises or simulations, to work on policy topics and vice versa. Discussion-based exercises can also be used to discuss technical issues. A general understanding of the technical environment and the impact of cybersecurity incidents is also necessary for policy-based cybersecurity exercises.

Cybersecurity exercises can serve technical, policy, legal, educational, or communication purposes, sometimes simultaneously, and focus on the tactical, operational, or strategic level of decision-making. Different types of cybersecurity exercises can further be applied to various target groups of participants and can even be combined. Cybersecurity exercises can, for example, enable decision-makers to "test existing emergency plans, target specific weaknesses, increase cooperation between different sectors, identify interdependencies (...). Cyber exercises are [also] important instruments to assess preparedness of a community against (...) cyber-attacks and emergencies."[20] The international cyber defense exercise, Locked Shields,[21] organ-

ized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), is an example of exercise that combines technical decision-making and defense of national IT systems with other purposes, such as strategic decision-making.[22] While Locked Shields is targeted at military personnel and strategic decision-makers, the Cyber 9/12 Strategy Challenge,[23] developed by the Atlantic Council, focuses purely on policy. It challenges students to think of potential courses of action and, thus, policies to mitigate an international cyber incident.[24]

Different types of cybersecurity exercises with different purposes and target groups offer great potential as training instruments tailorable to specific needs. However, unlike other more traditional instruments applied in policy work, such as awareness activities or setting IT security standards,[25] it can be challenging to understand the field and grasp the instrument's potential for a particular purpose for policy work. As with other policy instruments, a certain level of methodological expertise, such as choosing the right exercise types for the targeted purposes, is necessary. Cybersecurity experts are often unfamiliar with exercises as tools for cybersecurity policy, and experts on exercises might not be aware of cybersecurity-related matters.[26] The cybersecurity exercise types being used should not prevent decision-makers unfamiliar with the instrument from considering implementing them in the cybersecurity policy life cycle. A clear understanding of the different cybersecurity exercise types and their differences in use helps cybersecurity exercises gain more recognition as instruments for policy work.

2. Cybersecurity Exercise Types and Defining Features

Each cybersecurity exercise type, from cyber wargames to simulations, has certain defining features that highlight its advantages and emphasize differences between cybersecurity exercise types.

Red Team/Blue Team

Red team/blue team exercises are interactive cybersecurity exercises used to simulate attacks. The goal is to assess an "organization's existing security capabilities and identify areas of improvement in a low-risk environment"[27] and, thus, test technical systems and operational techniques, tactics, and procedures in incident response and cyber operations. The red team acts as an adversary and aims to compromise target systems. The blue team is a defender aiming to "identify, assess and respond to the intrusion."[28] Red team/blue team exercises' target groups are usually government, military, or private-sector entities using these exercises to test technical attack and defense processes. The exercises have the defining feature of **compromising systems that test whether the defense is good enough** and **explore potential weaknesses.**

> **Red team/blue team exercises for policy work – the author's example:** Red team/blue team exercises mainly test technical systems (for example, their effectiveness). Testing systems ultimately also tests the underlying policies that aim to protect the systems.

Cyber Wargames

Cyber wargames explore "how human decisions relate to cyber actions and effects."[29] These wargames can be "categorized as games with cyber and games about cyber[30]." Generally, wargames are "analytic games that simulate aspects of warfare at the tactical, operational, or strategic level. They are used to examine warfighting concepts, train and educate commanders and analysts, explore scenarios, and assess how force planning and posture choices affect campaign outcomes."[31] While wargames traditionally come from a military context and focus on the military's involvement in conflict, cyber wargames are often used beyond the military context and by other stakeholders. Cyber wargames have to consider specific aspects of cyberspace; for example, most of the technology is owned privately. Therefore, the

main target groups of cyber wargames are government, military, and business officials who use this cybersecurity exercise to improve strategic human decision-making. Moreover, they are also used by other stakeholders, for example, universities, to offer students an active learning experience to learn about cyber defense tools. Cyber wargames have several defining features that differentiate them from other exercise types: They particularly focus on **attack and defense scenarios.** Its core is the **idea of a conflict or rivalry with (often) geopolitical implications between different entities**. Therefore, they have a broader focus than red team/blue team exercises, which test technical attack and defense processes rather than focusing on the strategic decision-making context.

> **Cyber wargames for policy work – the author's example:** Cyber wargames, as a special type of wargame, are particularly useful to look at hypothetical gaps in future policy in the context of cyber defense. This does not only apply to the military but also the private sector. In cyber defense, the private sector is responsible for defending its systems. Hence, the private sector needs to analyze its cyber defense posture in a geopolitical context similar to how the military does in traditional wargames. On a strategic level, cyber wargames can also compare different policies and hold them against each other. Private sector entities also apply cyber wargames to, for example, think strategically about potential market shifts or competitors' actions. Cyber wargames are also useful for determining how certain cybersecurity components or factors influence existing policies or defense strategies.

Workshops

Workshops offer the opportunity "to hold constructive discussions during which [participants] work through a theoretical scenario, considering implications, procedures, interdependencies, and decisions."[32] Workshops are, thus, for example, used by academia, civil society, or government entities, which constitute the target group, to develop policies and procedures. Workshops exhibit a number of defining features: They are **speculative, collaborative**, and **open-ended** and can improve **understanding between different actors**; thus, they even offer the opportunity to **break up silos**.

> **Workshops for policy work – the author's example:** With regard to policy work, workshops can be used to identify problems and their implications. Due to their discussion-based nature, they also allow room to break up silos between different stakeholders and look at a scenario from different angles. Workshops offer a setting within which to discuss policies, learn from the exchange with others, and develop new ideas and policy options.

Tabletop Exercises

Tabletop exercises are defined as discussion-based exercises in which participants play fictional roles or assume the roles they have in real life; they "gather to work through a [hypothetical] scenario and existing procedures for responding to it. Typically, a facilitator will guide them through, with participants assuming specific roles and describing the steps they take and the decisions they make as the scenario unfolds. Such exercises are particularly useful for ensuring preparedness and familiarity with the procedures."[33] Tabletop exercises are, for example, run by government actors or civil society organizations to practice responsibilities and clear communication in the event of a cyber incident, among other purposes. The following features define tabletop exercises: They entail a **hypothetical scenario** constructed as realistically as possible. They offer a very effective means of **identifying responsibilities in a cyber incident**. Tabletop exercises **assist in exploring those responsibilities.** Therefore, private sector companies and critical infrastructure owners and operators also run internal tabletop exercises focusing on cybersecurity to ensure they know who is responding and what their responsibilities are.

> **Tabletop exercises for policy work – the author's example:** Tabletop exercises are suitable for finding and demonstrating specific policy problems, particularly because participants usually play their real-life roles. Tabletop exercises are also used to develop and test processes or specific policies to see who takes on which responsibilities. Decision-makers can, for example, use tabletop exercises to test staff members' compliance with policies.

Simulations

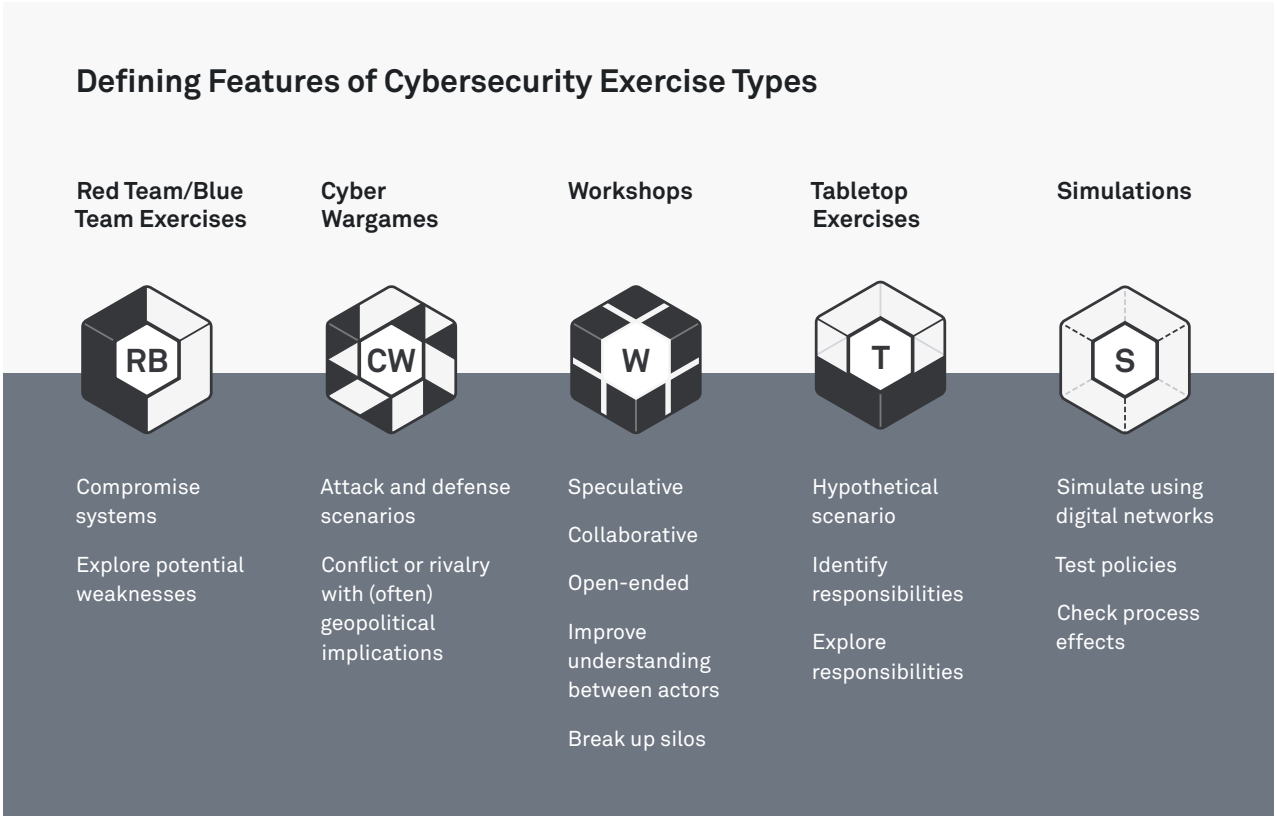
Simulations are cybersecurity exercises that "replicate real world situations,"[34] meaning that participants are exposed to scenarios to make them react or respond to them. These scenarios might be similar to real-world events or entirely fictional ones but are constructed as authentically as possible. Simulations also entail environments with a "virtual or secured digital network in which to conduct exercises using real tools and techniques,"[35] making them even more realistic and differentiating them from other exercises such as tabletop exercises. With a digital network, the experience is as close to a real event as possible.

Simulations are used, for example, by the government, private sector, or academia to improve communication, cooperation, and procedures. Simulations have several defining features. They **simulate reality as much as possible using a "virtual or secured digital network."**[36] They allow for testing specific hypotheses and **playing out unexpected events or responses in a safe environment**. Simulations are also useful

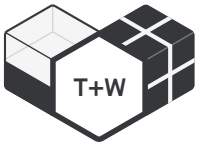
for learning how **one step in a process affects the next**. Additionally, (parts of) the simulation can be replayed under different conditions to investigate different outcomes. It must be well understood that their value is directly linked to the "reality" and complexity grade of the underlying simulation model.

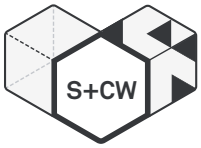
Simulations for policy work – the author's example: Simulations offer the possibility of testing processes and current policies by using a "virtual or secured digital network"[37] and simulating reality. In contrast to red team/blue team exercises or tabletop exercises, simulations allow for policy testing using a virtual model of networks and including technical tests while simultaneously allowing for the testing of operative or strategic questions. It is also possible to operationalize policy objectives through simulations and, for example, determine the time and resources necessary to fulfill certain policy objectives. Simulations can also show how the policy response impacts the technical response.

Defining Features of Cybersecurity Exercise Types



2.1 Cybersecurity Exercise Types – Mix and Match





Each cybersecurity exercise type has defining features and respective advantages, which make certain cybersecurity exercise types more useful for certain policy purposes than others. However, different types of cybersecurity exercises can also be used complementarily. This permits decision-makers to benefit from their combined features. Decision-makers might, for example, decide to plan the subject matter and structure of a **tabletop exercise in a pre-exercise workshop**. This way, they will benefit from the open-ended nature of the workshop format for planning the tabletop exercise and from the feature of tabletop exercises to work on hypothetical scenarios constructed as authentically as possible. Another example of complementary use is combining **cyber wargames and simulations**. Decision-makers can, for example, apply cyber wargames to identify weaknesses in their defense strategies and use simulations to make the exercises as real as possible using a "virtual or secured digital network."[38]

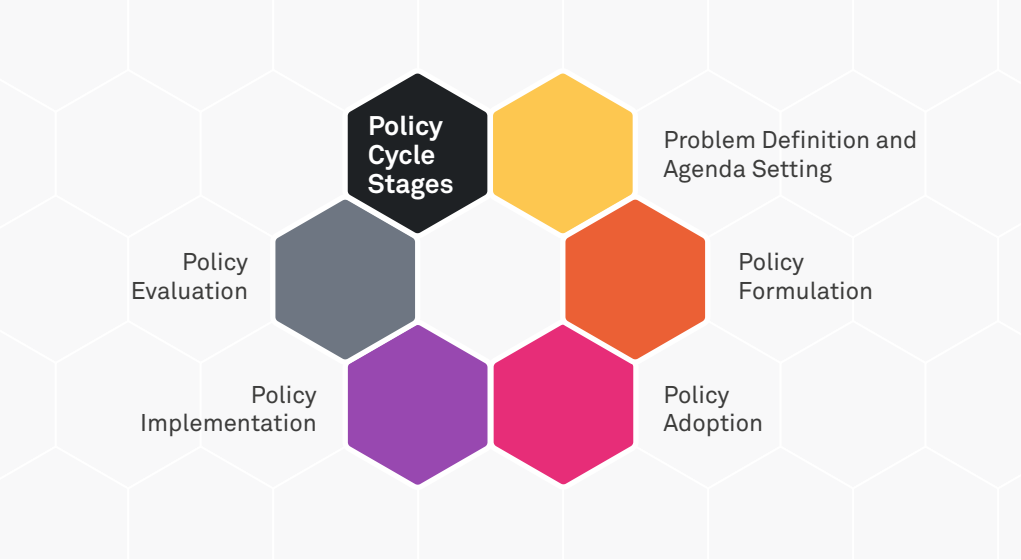
In addition to the complementary use of cybersecurity exercises, it is possible that the respective features of exercise types can overlap and are, thus, not completely distinct from one another. Cyber wargames and red team/blue team exercises have similar features. For example, both exercises focus on attack and defense scenarios. Since some features overlap, it helps look at each cybersecurity exercise type's defining features for specific guidance.

Therefore, the use of cybersecurity exercises for policy work not only includes single exercise types but also how to combine them, if suitable, and how to benefit from their combined features. To better explore their features, the following section assigns the cybersecurity exercise types to different stages of the policy cycle. This approach can show how their different defining features are used to achieve various policy work goals in the respective stages.

3. Cybersecurity Exercises and the Policy Cycle

After introducing different cybersecurity exercises and their defining features, it is worth examining potential applications for different cybersecurity exercise types along the policy cycle. This enables a better understanding of use cases for policy work and shows that cybersecurity exercises can achieve policy objectives and also to also develop policy.

The policy cycle consists of (1) "problem definition and agenda setting," (2) "policy formulation," (3) "policy adoption," (4) "policy implementation," and (5) "policy evaluation[39]." This chapter addresses the use of cybersecurity exercises in each stage.



Each policy cycle stage serves different purposes. Hence, the uses of different cybersecurity exercise types vary. Through hypothetical use cases, the different types are explored along the cycle. The use cases are not exhaustive due to the versatile nature of cybersecurity exercises as an instrument. Moreover, they provide a means to examine the potential of one particular cybersecurity exercise type for each respective stage of policy work. The different cybersecurity exercise types are discussed separately to highlight their individual benefits. Hence, one should consider that it is, of course, possible to combine different cybersecurity exercise types, as shown in chapter 3.1, to benefit from their combined features. Decision-makers will generally be able to identify where their policy work purpose can be played on the policy cycle. Exploring this is useful for guiding decision-makers to potential cybersecurity exercises that could be used to achieve the policy work purpose. This means that decision-makers can start at any stage and, from there, identify a cybersecurity exercise type that works best for their policy work.

3.1 The "Problem Definition and Agenda Setting" Stage

The "problem definition and agenda setting" stage consists of two phases: The first phase focuses on identifying problems, while in the second phase, these problems are assigned relevance for action. This means that some topics are placed on the (political) agenda and, therefore, addressed by the government, while others are not.[40] Different stakeholders can also use the "agenda setting" phase to put their topics and ideas on the agenda. Because of two different objectives followed at this stage, the respective objective of each use case is highlighted. Due to their defining features (1) red team/blue team exercises, (2) cyber wargames, and (3) workshops are particularly useful at this stage for supporting the main objectives in this policy phase, problem definition and agenda setting, by creating awareness of the underlying problems.

Red Team/Blue Team Exercises

Red team/blue team exercises are particularly beneficial at this stage for identifying systemic weaknesses in digital systems and identifying whether these weaknesses occur due to current policies.

Hypothetical Use Case

"Demonstrating Infrastructure Weaknesses Resulting From Missing Or Inadequate Policies": Identifying weaknesses or vulnerabilities in systems can be done by giving attackers, played by participants of the exercise, the opportunity to attack the system. As part of this stage of the exercise, the red team could, for example, try to compromise critical national infrastructure components. Naturally, it is better to detect weaknesses as early as possible. Participants are then asked to what extent the weaknesses are due to missing/inadequate policies. This is why red team/blue team exercises should already be used at such an early stage of the cycle: Only by demonstrating existing weaknesses, which equal problems, can decision-makers mitigate these weaknesses in the long run by, for example, adjusting policies.

Cyber Wargames

Cyber wargames can be applied to the policy cycle's "problem definition and agenda-setting" stage as they offer the analytical means to think through attack and defense scenarios while (often) considering geopolitical implications, helping to identify problems and set them on the agenda. Regarding current and historical scenarios, cyber wargames are tools that permit decision-makers to understand the status quo to better prepare for an unknown future or learn from the past.

Hypothetical Use Cases

"Demonstrate Potential Resource Problems": One can use cyber wargames to identify problems that could arise by playing through conflict scenarios, for example, a cyber espionage operation on critical infrastructure networks. Defenders, such as critical infrastructure owners or providers, can explore different responses to such attacks targeting their systems. By doing so, they can determine the extent to which their defense strategies and capabilities can respond to attack scenarios. For example, it might become clear that personnel, knowledge, experience, and skills are inadequately prepared to respond to possible attacks. Therefore, cyber wargames are also a means of thinking through conflict scenarios to prepare defenses.

"Discussing the Role of The Military": Most cyber incidents are below the threshold of armed conflict, and when it comes to large-scale incidents, military involvement is not clearly defined in all countries. Moreover, in some countries, the military needs to work with civilian organizations to prevent and respond to cyber incidents. At the "agenda-setting" phase, cyber wargames can define different stakeholders' roles, beyond the military, in national defense. This is increasingly important considering the prevalence of non-combative techniques, such as disinformation campaigns by threat actors. A cyber wargame helps increase awareness about open strategic questions, for example, regarding the role of private sector entities for national defense, and eventually pushes policymakers to reflect on solutions. This process contributes to emphasizing the urgency of the problems identified. By including senior decision-makers in the process, those open questions are put on the agenda.

Workshops

Workshops are applied at the "problem definition and agenda-setting" stage of the cycle to understand and analyze emerging problems. Due to their collaborative, discussion-based nature, participants can use this type of exercise to identify cybersecurity policy landscape problems and define the most pressing ones. The discussion-based workshop process offers the opportunity to define problems further and prioritize them by importance.

Hypothetical Use Case

"Identifying and Prioritizing Problems": A country that undergoes digital transformation may not have clearly defined what kind of cybersecurity problems come with it. In this case, a workshop is used to examine different theoretical scenarios for dealing with digital transformation issues. The format allows for a safe space that gives room for thought exper-

iments and speculative ideas, broadening the perspective on a specific topic. Participants could, for example, examine how the distribution of information and communication systems lead to new vulnerabilities for business or government systems. They could also map vulnerabilities and possible attack vectors targeting these vulnerabilities as a foundation for better preparedness.

3.2 The "Policy Formulation" Stage

Once the problems are defined, prioritized, and put on a decision maker's agenda, the next stage in the policy cycle is "policy formulation." The "policy formulation" stage "deals with the elaboration of alternatives of action (...)"[41] and "involves the definition, discussion, acceptation or rejection of feasible courses of action for coping with policy problems."[42] This includes writing policy proposals and defining policy objectives and suitable policy instruments.[43] Due to their defining features, it is particularly effective to implement the following exercises at this stage: (1) cyber wargames, (2) workshops, (3) tabletop exercises, and (4) simulations. These exercise types contribute to the main goal in this policy phase: to clarify the details of a respective policy.

Cyber Wargames

At this stage, cyber wargames may be applied to elaborate on courses of action involving cybersecurity incidents in conflict or below the threshold of conflict to tackle problems defined or put on the agenda in the previous policy cycle stage. Through cyber wargames, different players' roles can be discussed and defined in detail.

Hypothetical Use Case

"Interdependencies Clarified": Decision-makers may have realized that there is an interdependence between civil and military actors involved in responding to a conflict situation that needs to be further defined through policies. Decision-makers can now apply cyber wargames to think through solutions and address unclear interdependencies. At this stage, cyber wargames specifically offer the opportunity to play through response scenarios in which the military relies on civil actors or vice versa. Through this, participants can realize how new policies need to be formulated, for example, what information-sharing policies must be implemented.

Workshops

At this stage, workshops can be particularly useful for breaking up silos between actors. For example, in election security, which relies on the cooperation of many stakeholders inside and outside of the government, using workshops for policy formulation can create cooperation and enable the inclusion of different suggestions from all parties before policies are even written. Workshops offer the possibility of creating mutual understanding – for example, through letting participants discuss their roles and considering different solutions for one problem.

Hypothetical Use Case

"Who Does What in Election Security": Decision-makers could, for example, plan a multi-stakeholder workshop with participants from the government, civil society, academia, and the private sector to discuss how to improve election security as a joint effort between public, private, and civil institutions.[44] The foundation of such discussions could, for example, be a hypothetical scenario of a cyber operation on election infrastructure. Discussing this scenario would help stakeholders understand what everyone's role is and gather the knowledge for solutions from different sectors. Through such an exercise, policies for more effective cooperation between public, private, and civil institutions could be formulated – for example, how to best protect the accounts of politicians by creating policies of cooperation between the government and major tech companies for prevention strategies and in case of incidents. Decision-makers can, thus, analyze ways of tackling a problem that is identified and talk through policy options that might not be brought to the table in other environments or circumstances without involving a number of different stakeholders talking through the same scenario.

Tabletop Exercises

At this stage, tabletops can be used to formulate a clear strategy by playing through different scenarios and assigning different responsibilities and their impact along the way. The discussion-based nature of tabletop exercises helps decision-makers understand where roles and responsibilities could lie in an incident. The lessons that are drawn from the exercise can then contribute to shaping the policy.

Hypothetical Use Case

"Working on Incident Response": Decision-makers from the government or private sector could, for example, use a tabletop exercise to develop an incident response plan with clearly defined responsibilities. The key element of the plan is the clear assignment of roles and responsibilities to stakeholders, which might vary and change in the exercise to determine

what impact the assignment of different lead responsibilities has in case of an incident. Tabletop exercises can allow decision-makers to determine where roles and responsibilities should reside. In the same context, decision-makers could also use tabletop exercises to identify the threshold when an incident response plan becomes active and what or who would trigger it. This ultimately helps to improve and finalize an incident response plan by extracting lessons learned from the exercise.

Simulations

Simulations can be used at this stage to assess how a cybersecurity policy changes specific factors or circumstances. When discussing how a particular policy could look at this stage of the cycle, simulations can also be used to operationalize resources needed to achieve policy objectives and assess what effects certain policy changes would have due to its ability to simulate a real-world environment as much as possible. During simulations, it is possible to adjust the controls to see different outcomes or impacts of the cybersecurity policy. Simulations allow participants to play roles other than their profession to make stakeholders experience a cyber incident from a different perspective. This can improve cooperation and communication between stakeholders, such as those from different sectors. This may enable them to better understand other actors' needs in certain situations.

Hypothetical Use Case

"Pre-testing a Policy Instrument": When formulating a detailed policy, decision-makers must be aware of the resources required to implement the respective policy and fulfill certain objectives. For example, suppose a national government aims to create security mechanisms that protect the election infrastructure proactively, such as implementing a penetration test. Government officials could simulate a penetration test of a virtual representation of the specific election's infrastructure. That way, decision-makers can better assess how much time or which specific skill sets a penetration test needs. A simulation could reveal that the government lacks specialists who understand the threat landscape and potential risks to the government systems. This finding could then lead to policy formulation adaptations, such as including adjusted training for staff members. It could even lead to choosing a different policy instrument than that used in the simulation if it did not meet the expected objectives.

3.3 The "Policy Adoption" Stage

After the policy has been formulated, the responsible institutions, such as legislative or executive bodies,[45] must approve and adopt it. For instance, adoption decisions depend on party affiliation or a specific policy's costs and benefits.[46] This stage demands support to be secured; a majority or consensus among actors is necessary to adopt the policy. Due to their defining features, (1) cyber wargames and (2) tabletop exercises are particularly effective to implement at this stage. These exercise types can contribute to this policy phase's main goal: a formulated policy's final adoption or approval.

Cyber Wargames

Cyber wargames are particularly useful to implement at this stage of the policy cycle as they can contribute to bringing a policy dealing with (geopolitical) conflict to final approval. Decision-makers can use cyber wargames to play through scenarios, focusing particularly on showing stakeholders how the policy and its elements work. Doing so can convince them of a policy's benefits, for example, by showing how the outcome differs from the current policy's potential responses. Ultimately, this can contribute to majority and consensus-building. This is particularly important for (cyber) conflict policies due to their potentially grave geopolitical implications, interdependencies on different sectors and stakeholders, and potential links to other domains. Cyber wargames also offer opportunities to extract lessons learned to finalize the policy.

Hypothetical Use Case

"Reaction to Cyber Incidents by the Military": Suppose a country was already in conflict with another state and has now been attacked by its cyber operation. A new policy is on the table: reacting with traditional means of warfare to this cyber attack when in conflict. Using wargaming can help one explore how adopting this new policy affects strategic posture and the possible risk of escalation. It also allows discussions on how the new policy could impact current policies, strategies, and processes that are already implemented, such as applying international law and norms in this regard.

Tabletop Exercises

At this stage of the policy cycle, tabletop exercises can bring a policy forward for final adoption due to their defining feature, which allows the participants to play through how responsibilities would work in a cyber incident. A tabletop exercise that includes decision-makers who have to implement the policy could show how the policy will work, bring the response process to life, show policy features, and dis-

cuss how it differs from the status quo. Decision-makers can also just shadow such an exercise to see the potential impact of changing a policy. Exploring a policy this way allows for a better understanding of its features and intentions. This is particularly useful because different bodies might be responsible for drafting and making decisions about a policy.

Hypothetical Use Case

"Testing a Vulnerability Management Process": A government disclosure decision process (GDDP), also known as a vulnerabilities equities process (VEP), involves many parties, from governmental actors to potential advisors, the private sector, and more[47]. Through the formulation process, the body drafting the policy might have consulted all of these parties. To gain final approval, however, it might be useful to play through different cases. This will allow stakeholders to experience the process for concrete (edge case) vulnerabilities before it is passed because the devil is in the details with such processes,[48] and new concerns might have arisen since the parties were last consulted. Running a tabletop exercise on a draft GDDP/VEP is therefore helpful for addressing final concerns, gathering support, or even coming to the conclusion to go back to the drawing board ("policy formulation" stage).

3.4 The "Policy Implementation" Stage

Once the policy's details are clarified, the policy needs to be implemented. At the "policy implementation" stage of a specific policy, all factors that hinder or favor a smooth implementation must be considered. Policies, laws, and regulations are translated into concrete facts, steps, or material achievements.[49] Due to their defining features, (1) red team/blue team exercises, (2) tabletop exercises, and (3) simulations can strengthen the implementation process.

Red Team/Blue Team Exercises

At this stage, red team/blue team exercises are applied to analyze and test the policy and its underlying processes that have just been implemented and identify factors that may hinder the successful policy implementation.

Hypothetical Use Case

"Password Protection Implementation Check": Shortly after its implementation, decision-makers could, for example, use red team/blue team exercises to test whether staff members have implemented new password protection procedures to increase the IT security of laboratories for vacci-

ne development.[50] If they were not implemented correctly, red team/blue team exercises might help decision-makers determine why.

Workshops

At this stage, workshops can identify the important stakeholders responsible for implementing policy in certain incidents. The discussion-based and speculative format helps decision-makers talk through different scenarios, map out responsibilities, and examine what policies would be implemented. This can be useful to do before designing a specific exercise with the target audience, who would implement policies in reality.

Hypothetical Use Case

"Who Would Need To Train This Incident?": Workshops can be used before implementing another exercise, for example, a tabletop exercise, to see whether everyone knows their responsibility. It is a good way to find the right people who need to be in the room for a certain exercise to be effective. A workshop is discussion-based; hence, it is a great way to explore a scenario with different experts and analyze who would be affected by a certain incident and who would need to work together. One cannot test whether the identified parties would work together but can prepare such cooperation through the workshop.

Tabletop Exercises

Tabletop exercises are beneficial at the "policy implementation" stage as they can check stakeholders' familiarity with existing policies and procedures. This is due to their discussion-based format, allowing participants to talk through the different policy options on the table using existing policies and strategies. The discussion-based format also provides for assessment steps taken during the implementation process. It may increase the understanding of the responsibilities of other stakeholders responding simultaneously and where interdependencies come into play.

Hypothetical Use Case

"Educating On Policies And Responsibilities": At the stage of "policy implementation," tabletop exercises can be set up as educational, multi-stakeholder exercises. Decision-makers could use them to clarify whether stakeholders, for example, from the private sector, civil society organizations, and government entities are aware of a certain policy in the first place. After that, they could assess if the participants involved, such as a certain government entity's staff members, know about and understand their responsibilities in the context of a newly implemented policy.

Simulation

The "policy implementation" stage also benefits from simulations. Simulations may be used at this stage to test policy and to ensure correct policy implementation. The difference between tabletop exercises and simulations when testing policy at this stage is that simulations offer means to test policies using "virtual or secured digital network,"[51] making the interaction between the technical and the strategic response more real. Thus, stakeholders can see a policy's impact on the technical level and in other stakeholders' responses. As simulation controls can be adjusted, a policy also can be tested during the implementation phase under different conditions.

Hypothetical Use Cases

"Implementing The Disaster Response Plan": If, for example, corporate decision-makers recently implemented a disaster recovery plan for continuing their mission-critical processes after a cyber incident, they could test this new policy's compliance. Simulating a cyber incident on their business systems may help decision-makers understand if and how employees follow the plan, for example, by activating the Emergency Response Team and the Disaster Recovery Team right after the incident.[52] Simulations replicate reality as much as possible using a "virtual or secured digital network,"[53] making them cybersecurity exercises that effectively allow participants to, for example, experience policy non-compliance's impact.

"Identifying Problems In Policy Implementation": Simulations are also beneficial for working on implementation problems. When implementing national response processes in cyber operations, decision-makers can, for example, use simulations to see which factors hinder policy implementation in a specific case. These factors usually become apparent in different scenarios. For example, an IT security personnel shortage could hinder effective response processes, particularly if a country suffers from multiple, simultaneous attacks. Another example of a hindrance to implementation is the stakeholders' compliance with a policy. When implementing a national response process, government entities must wait for an initial forensic examination of a cyber operation before taking further action. A simulation offers a safe environment for assessing whether this process is understood and followed and, if not, why.

3.5 The "Policy Evaluation" Stage

A policy proceeds to the "policy evaluation" stage after implementation. As its name suggests, this stage evaluates policies and actions taken (for example, by the government) that have previously passed through the policy cycle.[54] However, due to its nature, a policy might loop back to the "problem definition" stage if a new problem is identified during the evaluation. Due to their defining features, (1) red team/blue team exercises, (2) workshops, (3) tabletop exercises, and (4) simulations are particularly effective to implement at this stage.

Red Team/Blue Team Exercises

At this stage, red team/blue team exercises are applied to test policies. The difference to prior applications, particularly to the use of red team/blue team exercises in the "policy implementation" stage, is that the respective cybersecurity policy has already been in place for some time. Therefore, the exercise evaluates the policy rather than how well it was implemented.

Hypothetical Use Case

"Responding With Existing Policy To New Attack Types": A policy's effectiveness can be evaluated by having a red team apply new forms of attacks, with the blue team responding them. Such new forms of attacks can be related to the evolution of cybercrime. Cybercriminals used to only encrypt files; nowadays, they also copy data and delete backups. This is done to increase pressure and blackmail victims. Observers may find that the blue team's responses are no longer applicable to these attacks. While a cybercriminal's encryption can be mitigated by creating backups, this approach does not work if copied data and backups are deleted. These findings could then show that decision-makers need to update their respective policies.

Workshops

At the "policy evaluation" stage, workshops evaluate whether an existing policy is sufficient, needs to be amended, or whether a new policy should be introduced due to their collaborative, discussion-based, and open-ended nature.

Hypothetical Use Case

"Evaluating Existing Policy and Contemplating New Ones": After implementing new policies, such as those addressing problems resulting from digital transformation, decision-makers might organize a multistakeholder workshop to evaluate the status quo. They could ask participants from different societal sectors whether they believe that the existing policy is

sufficient to address challenges, such as those resulting from deploying information and communication systems, leading to new vulnerabilities. If workshop participants decide that these challenges are inadequately addressed, the workshop will help identify the need for new policies.

Tabletop Exercises

The "policy evaluation" stage further benefits from tabletop exercises, which can assess and test policies, for example, regarding their effectiveness.

Hypothetical Use Case

"Changing Threat Landscape": An example of using tabletop exercises for evaluation purposes would be to assess whether a cyber response policy is appropriate for a changing threat landscape. The cyber threat landscape may change due to situations such as new actors using malicious tools or different tactics. Decision-makers would need to evaluate whether their existing defense policies would still apply or need adaptation. Some cybercriminal groups are now not just encrypting data but also threatening to publish the data. Hence, business decision-makers must ask whether the protection policy is useful in such a case. Backups alone may not be enough. Thus, such a scenario may assist in exploring to what extent the policy needs evaluation.

Simulations

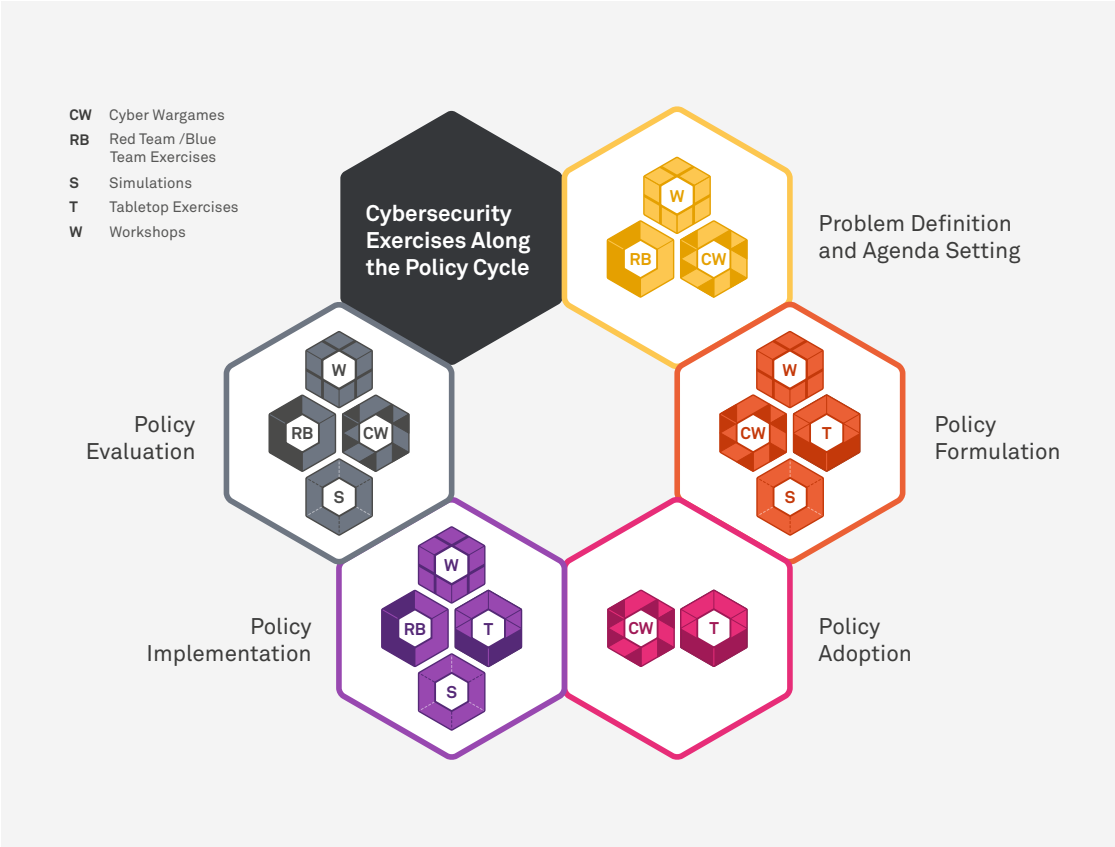
At the "policy evaluation" stage, simulations can be used to test policies. Contrasting discussion-based exercises, such as tabletop exercises, simulation test policies are based on a "virtual or secured digital network"[55] and enable decision-makers to replicate reality.

Hypothetical Use Case

"Information Sharing Across Levels": Decision-makers could, for example, apply simulations to test EU-level cooperation processes. Thus, the simulation would test the cooperation between key national cybersecurity institutions and EU institutions, and the findings would feed into the new policy's overall evaluation. For example, national responsibilities might have shifted since implementation, resulting in a policy changing. The virtual or secured digital network also permits an evaluation of how the policy response could affect different cooperation levels. It could, for example, evaluate whether the information exchange on a strategic level works as defined in the policy.[56] By testing this, the policy can be evaluated.

The discussion shows that different cybersecurity exercises, from cyber wargames to tabletop exercises, can be used for policy work, such as pol-

icy-making, and to achieve policy objectives throughout the policy cycle stages. To use exercises to their full potential, it is helpful to consider the policy work's scope (the policy work's goal and the target audience) and in which policy cycle stage the policy work can be placed. Answering these questions guides decision-makers to certain types of cybersecurity exercises and helps them understand how their defining features can be used depending on the stage. This approach helps to determine exercise types for particular purposes. Thinking through each exercise's defining features then helps participants pick the best one for their purpose and available time.



4. Case Study: Exploring Cybersecurity Exercises for Stiftung Neue Verantwortung

The international cybersecurity policy team at Stiftung Neue Verantwortung e. V. (SNV) uses cybersecurity exercises for policy work at the "problem definition and agenda-setting" stage and the "implementation phase" of the policy cycle. Those are just two examples of how exercises can be used for policy work in think tanks.

4.1 Workshops to Put Election Security Threats and Policies on the Agenda

As a think tank, one of SNV's main tasks is to analyze the extent to which technology could impact society. Traditionally, SNV examines technological development's impact on elections through expert workshops and desk research, resulting in, for example, the publication of the study "Securing Democracy in Cyberspace."[57] After publication, it was soon noticed that it was important to increase the general awareness of new threats to elections and explore solutions not yet defined or implemented. This type of policy work was identified to be situated in the "problem definition and agenda setting" stage – using cybersecurity exercises as an instrument to make current and upcoming decision-makers, for example, in universities aware of the topic.

Using workshops as a cybersecurity exercise was deemed most appropriate for this purpose as it allowed participants from different sectors to explore the roles played in responses. It also allowed for discussing current policy options and how these could tackle new threats in the most collaborative and open-ended way. Workshops with current decision-makers aimed to put the problem of election security on the agenda and increase awareness about potential new policies required to meet the threat. For upcoming decision-makers in universities, the workshops were an instrument to educate on cybersecurity and specifically put election security on the study agenda. Most German universities do not cover those topics in their studies yet.

4.2 Workshops and (Virtual) Tabletop Exercises to Increase the Understanding and Impact of Policies

Another way to use cybersecurity exercises as a think tank is to implement a workshop on country-specific cybersecurity policies and stakeholders to identify existing policies and responsibilities among stakeholders. The discussion-based format

makes it easy for stakeholders to reflect, to progress from one topic to the next, not being confined to a scenario per se but rather to gather and share information. Moreover, the workshop can aid in talking through different ideas for a scenario and help identify a likely scenario and tasks for the following exercise. This information is then used to design and run a tabletop exercise that is as realistic as possible. Here, workshops and tabletop exercises complement each other, as tabletop exercises are based on hypothetical scenarios that are constructed as realistically as possible. The workshop part beforehand identified the topic, policies, and the stakeholders for the tabletop exercise. SNV then uses tabletop exercises to understand the effects of implementing existing policies through a specific scenario where responsibilities and clear communication in a cyber incident are practiced.

In the tabletop exercise, participants representing different sectors respond to an incident using existing policies to increase their understanding of the responsibilities and interdependencies among different stakeholders. By including stakeholders from the government, the private sector, and civil society the exercise allows participants to learn about the implementation's impact on other stakeholders' responses and see whether stakeholders comply with policies. Through interaction between participants, the interdependencies between different stakeholder groups become clear. In addition, the potential needs of specific stakeholders, such as clearer lines of command, may be revealed, leading to discussions on how the policies can be implemented better and more effectively.

At the "implementation" stage, tabletop exercises are conducted with the sole purpose of increasing the understanding of existing policies, their implementation, and impact. In the tabletop exercise, the following questions are asked: "How does the implementation of the policy affect the responses of other stakeholders?", "what has worked well?", and "why or how could the policy be implemented better?" The participating stakeholders train their own responses to existing policies, learn about the implemented policies, or give feedback to, for example, the governmental group focusing on whether the implemented policies are understandable.

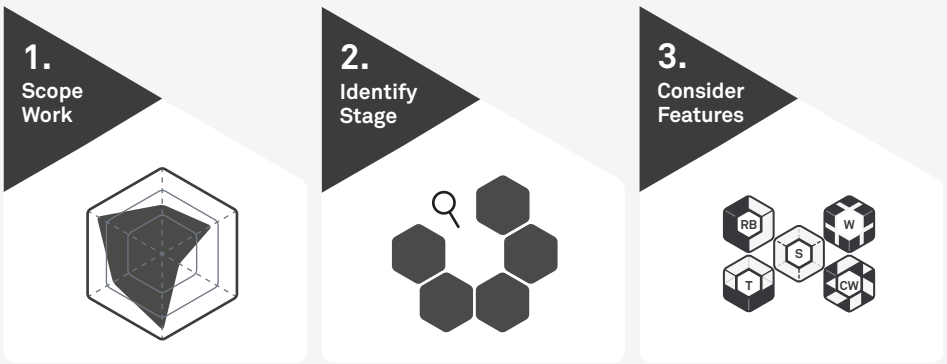
5. Guidance On Exploring Cybersecurity Exercises for Policy Work

Cybersecurity exercises are carried out for a variety of purposes. They can be a useful instrument for policy work (see "Cybersecurity Exercises and the Policy Cycle"). They can contribute to identifying problems with a policy that should be addressed, evaluating policies, or achieving policy objectives, such as increasing situational awareness among different stakeholders and identifying weaknesses in systems. The policy cycle stage during which the policy work occurs matters because the different cybersecurity exercise types can be applied differently, depending on the stage. They may also not be suitable for certain other stages or may work best in combination (see "Cybersecurity Exercise Types – Mix and Match"). Looking at the different exercise types by showing their defining features and analyzing their usage along with the policy cycle highlights that certain types are particularly beneficial to implement at certain policy cycle stages.

Exploring the potential application of cybersecurity exercises for policy work showed that this is an instrument that decision-makers should consider when developing cybersecurity policies and/or aiming to achieve different cybersecurity policy goals.

Since policy work applications are diverse, decision-makers are advised to explore cybersecurity exercises as potential policy work instruments by following these three steps:

3 Guidance Steps
Explore Cybersecurity Exercises for Policy Work



1. Scope Out the Policy Work

Consider the policy work you aim to do and the target audience you want to reach.

It is helpful to scope out the policy work first, for example, by looking at the goal or target audience before considering exercises as potential instruments to achieve the goal. Policy work can aim to achieve policy objectives and develop policies (further). When using exercises to achieve policy objectives, it is important to define those policy objectives clearly and know what stakeholders will be the target audience. An example is the goal of increasing situational awareness of cyber threats among small- and medium-sized enterprises. The goal should be achieved after applying an exercise (for example, increased awareness of small- and medium-sized enterprises). Before choosing exercises, knowing the goals and target audience is crucial for exploring whether other instruments are better suited.

Policy work can, however, also be the identification of a policy problem, the analysis of a problem, the development of the policy itself, or the evaluation of a policy. Here, exercises could be explored to do this policy work; the goal is to test staffer compliance on a specific response strategy within a business. In this case, the goal would be achieved if it is determined whether or not staffers comply with the policy.

Once the scope of the policy work is clear, decision-makers can move one step closer to knowing whether exercise is the best instrument to achieve their policy work goals.

2. Identify Stage Of Use

Identify where your policy work is best situated on the policy cycle.

This step identifies at what stage of the policy cycle the policy work is situated. The scope of the policy work mostly gives some clues on where the work is situated. When aiming to work on and test policy compliance, it is clear that the policy is already implemented. Therefore, it leaves the option to look for exercise types that can be applied in the “implementation” or “evaluation” phases of the policy cycle. Increasing situational awareness among small- and medium-sized companies can be explored at the start of the policy cycle. In the “problem definition” phase, exercises can assist small- and medium-sized companies in understanding the problems they are dealing with and increase their awareness without necessarily working on a con-

crete policy. Once the policy work is placed on the policy cycle, decision-makers can explore which exercise type in the chosen stage would be best suited.

3.

Consider The Defining Features For Your Needs
Which exercise type is the best to achieve the policy work goal?

At this step, becoming familiar with the defining features of each exercise type and how they could complement each other helps one pick the best exercise type(s) to achieve the policy work goal. For example, decision-makers may want to test if employees comply in the case of a cyber incident. A cyber incident is a technical event that a simulation can best represent due to its virtual or secured digital network, which constitutes its defining feature. Another example would be a case aimed at increasing awareness and prioritizing threats or solving problems for small- and medium-sized enterprises. A workshop may be the best fit for this subject matter because it allows for explorations and helps identify threats and learn about them. It also prioritizes which threats may affect the business and increase situational awareness.

About the Authors

Rebecca Beigel is a project manager for international cybersecurity policy at Stiftung Neue Verantwortung. Her work focuses on German cybersecurity policy and on cybersecurity exercises in country-specific contexts.

Julia Schuetze is a junior project director for international cybersecurity policy and has been with Stiftung Neue Verantwortung since 2017. Her expertise lies in the areas of EU cyber diplomacy with the USA and Japan, cyber operations against electoral processes and the shortage of IT security specialists in Germany. She also designs and implements cybersecurity policy exercises.

Contact the Authors

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

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

Endnotes

1 NIST, “malicious cyber activity”, Computer Security Resource Center, n.d., https://csrc.nist.gov/glossary/term/malicious_cyber_activity.

2 Bundesamt für Sicherheit in der Informationstechnik, “Die Lage der IT-Sicherheit in Deutschland 2020”, 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2; ENISA, “ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected”, ENISA, October 20, 2020. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.

3 Sven Herpig and Julia Schuetze, “Transatlantic Cyber Forum—Cooperating on Borderless Cyber Security Challenges”, Redesining Organizations, Springer International Publishing, 2018, https://www.stiftung-nv.de/en/publication/transatlantic-cyber-forum-cooperating-borderless-cyber-security-challenges.

4 Michael Daniel, “Why Is Cybersecurity So Hard?”, Harvard Business Review, 2018, https://hbr.org/2017/05/why-is-cybersecurity-so-hard.

5 Cf. Julia Schuetze,”Annex to EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals”, EU Cyber Direct, 2020, https://www.stiftung-nv.de/sites/default/files/rif_annex-eu-us-final.pdf.

6 Cf. Julia Schuetze,”Annex to EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals”, EU Cyber Direct, 2020, 62, https://www.stiftung-nv.de/sites/default/files/rif_annex-eu-us-final.pdf.

7 There are many cybersecurity exercise types, such as drills or capture-the-flag exercises. However, this paper focuses on what the author’s identified as the most common exercise types. It is also necessary to differentiate between technical cybersecurity exercises to train tactics, techniques and procedures (TTP) on a technical level and strategic focused cybersecurity exercises to evaluate policy and strategy. In the context of this paper, only the latter are addressed.

8 ENISA, “Latest Report on National and International Cyber Security Exercises”, ENISA, 2015, 17, https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises; Robert S. Dewar, “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, 2018, 6, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf.

9 ENISA, “Latest Report on National and International Cyber Security Exercises”, ENISA, 2015, 17, https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises;

Robert S. Dewar, “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, 2018, 6, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf.

10 Nina Kollars and Benjamin Schechter, “Pathologies of obfuscation: Nobody understands cyber operations or wargaming”, Atlantic Council, February 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/pathologies-of-obfuscation-nobody-understands-cyber-operations-or-wargaming/.

11 Robert S. Dewar, “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, 2018, 6, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf;

Gerard Prinsen and John Overton, “Policy, Personalities and Pedagogy: The Use of Simulation Games to Teach and Learn about Development Policy”, Journal of Geography in Higher Education, 2011, https://www.tandfonline.com/doi/full/10.1080/03098265.2010.548508?scroll=top&needAccess=true; Flavius Vegetius Renatus, “Epitoma rei militaris: Epitome of Military Science”, 2001, https://www.amazon.com/Vegetius-Liverpool-University-Translated-Historians/dp/B00RWSO0LS.

12 Robert S. Dewar, “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, 2018, 7, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf;

13 Ibid.

14 Ibid.

15 Generally, there are even more cybersecurity exercise types, such as drills or capture-the-flag exercises. However, this paper focuses on what the authors identified as the most common exercise types.

16 cf. ENISA, “Latest Report on National and International Cyber Security Exercises”, ENISA, 2015, 17, https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises;

17 Dr. Stefan Heumann und Philippe Lorenz, “Sechs Szenarien für Deutschlands Arbeitsmarkt”, Stiftung Neue Verantwortung, March 14, 2016, https://www.stiftung-nv.de/de/publikation/sechs-szenarien-fuer-deutschlands-arbeitsmarkt.

18 efp, “Scenario Method”, European Foresight Platform, n.d., http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/scenario/.

19 Robert S. Dewar, “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, 2018, 15, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf;

20 ENISA (2012): National Cyber Security Strategies Practical Guide on Development and Execution, 17.

21 CCDCOE, “Locked Shields”, n.d., https://ccdcoe.org/exercises/locked-shields/.

22 Ibid.

23 Atlantic Council, “Cyber 9/12 Strategy Challenge”, n.d., https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/.

24 Ibid.

25 Julia Schuetze, “EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals”, EU Cyber Direct, 49, https://eucyberdirect.eu/content_research/eu-us-cybersecurity-policy-coming-together-recommendations-for-instruments-to-accomplish-joint-strategic-goals/.

26 Nina Kollars and Benjamin Schechter, “Pathologies of obfuscation: Nobody understands cyber operations or wargaming”, Atlantic Council, February 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/pathologies-

of-obfuscation-nobody-understands-cyber-operations-or-wargaming/.

27 Crowdstrike, “Red Team vs Blue Team Cybersecurity Simulation Defined”, September 3, 2020, https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/.

28 Ibid.

29 Benjamin Schechter, “Wargaming Cyber Security”, War on the Rocks, September 4, 2020, https://warontherocks.com/2020/09/wargaming-cyber-security/.

30 Ibid.

31 RAND Corportation, “Wargaming”, n.d., RAND, https://www.rand.org/topics/wargaming.html.

32 ENISA, “Good Practice Guide on National Exercises Enhancing the Resilience of Public Communications Networks”, December 2009, https://webcache.googleusercontent.com/search?q=cache:PCKzS6Rig2EJ:https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide/at_download/fullReport+&cd=1&hl=de&ct=clnk&gl=de&client=firefox-b-e.

33 ENISA, “Good Practice Guide on National Exercises Enhancing the Resilience of Public Communications Networks”, December 2009, https://webcache.googleusercontent.com/search?q=cache:PCKzS6Rig2EJ:https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide/at_download/fullReport+&cd=1&hl=de&ct=clnk&gl=de&client=firefox-b-e.

34 Robert S. Dewar, “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, 2018, 15, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf.

35 Ibid.

36 Ibid.

37 Ibid.

38 Robert S. Dewar, “Cyber Security and Cyber Defense Exercises”, Center for Security Studies, 2018, 15, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf.

39 Sonja Blum and Klaus Schubert, “Politikfeldanalyse Eine Einführung”, Springer VS, 156.

40 Sonja Blum and Klaus Schubert, “Politikfeldanalyse Eine Einführung”, Springer VS, 161-175.

41 Christoph Knill and Jale Tosun, “Policy Making”, Chair of Comparative Public Policy and Administration Department of Politics and Management University of Konstanz, January 2018, 18, https://kops.uni-konstanz.de/bitstream/handle/123456789/3885/WorkingPaper2008_01.pdf?sequence=1&isAllowed=y.

42 Christoph Knill and Jale Tosun, “Policy Making”, Chair of Comparative Public Policy and Administration Department of Politics and Management University of Konstanz, January 2018, 13, https://kops.uni-konstanz.de/bitstream/handle/123456789/3885/WorkingPaper2008_01.pdf?sequence=1&isAllowed=y.

43 Ibid, 13-14.

44 Cf. Sven Herpig and Julia Schuetze, “Securing Democracy in Cyberspace: An Approach

to Protecting Data-Driven Elections", Stiftung Neue Verantwortung, 2018, https://www.stiftung-nv.de/en/publication/securing-democracy-cyberspace-approach-protecting-data-driven-elections.

45 European Geosciences Union, "The policy cycle", n.d., https://www.egu.eu/policy/basics/cycle/.

46 Christoph Knill and Jale Tosun, "Policy Making", Chair of Comparative Public Policy and Administration Department of Politics and Management University of Konstanz, January 2018, 16-17, https://kops.uni-konstanz.de/bitstream/handle/123456789/3885/WorkingPaper2008_01.pdf?sequence=1&isAllowed=y.

47 see Sven Herpig, Ari Schwartz" The Future of Vulnerabilities Equities Processes Around the World", 2019, Lawfare https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world and Sven Herpig, Governmental Vulnerability Assessment and Management Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities, 2018, Stiftung Neue Verantwortung https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf

48 https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf

49 Bundeszentrale für politische Bildung, "Implementation", based on Klaus Schubert, and Martina Klein: Das Politiklexikon, 2018, https://www.bpb.de/nachschlagen/lexika/politiklexikon/17624/implementation; Sonja Blum and Klaus Schubert, "Politikfeldanalyse Eine Einführung", Springer VS, 190-195.

50 Cf. National Academy of Sciences, "Prudent Practices in the Laboratory: Handling and Management of Chemical Hazards: Updated Version", 2011, https://www.ncbi.nlm.nih.gov/books/NBK55881/.

51 Robert S. Dewar, "Cyber Security and Cyber Defense Exercises", Center for Security Studies, 2018, 15, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf.

52 Cf. Micro Focus, "IT Disaster Recovery Planning: A Template", n.d., https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf

53 Robert S. Dewar, "Cyber Security and Cyber Defense Exercises", Center for Security Studies, 2018, 7, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf.

54 Bundeszentrale für politische Bildung, "Evaluierung/Evaluation", based on Klaus Schubert, and Martina Klein: Das Politiklexikon, 2018, https://www.bpb.de/nachschlagen/lexika/politiklexikon/17469/evaluierung-evaluation.

55 Robert S. Dewar, "Cyber Security and Cyber Defense Exercises", Center for Security Studies, 2018, 15, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf.

56 Cf. European Commission, "Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises", September 13, 2017, https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF.

57 Sven Herpig and Julia Schuetze, "Securing Democracy in Cyberspace: An Approach to Protecting Data-Driven Elections", Stiftung Neue Verantwortung, 2018, https://www.stiftung-nv.de/en/publication/securing-democracy-cyberspace-approach-protecting-data-driven-elections.

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

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Infographics and Layout:
Ulf Seißenschmidt
www.ulf-seissenschmidt.de

Free Download:

www.stiftung-nv.de