GLOBAL FORUM ON CYBER EXPERTISE

INTRODUCTION TO TABLETOP EXERCISES (TTX)

A PRACTICAL GUIDEBOOK FOR ORGANIZATIONS

PREPARED BY

Capgemini

AS PART OF

GFCE WORKING GROUP B ON CYBER SECURITY INCIDENT MANAGEMENT & CRITICAL INFRASTRUCTURE PROTECTION

MARCH 2023

Acknowledgements

The GFCE would like to acknowledge the work of the Project Team on 'Introduction to Tabletop Exercises (TTX): A Practical Guidebook for Organizations" of GFCE Working Group B Cyber Security Incident Management & Critical Infrastructure Protection. The Project Team led work on the survey and the report and included contributions from:

- Gerard Elfa García, Capgemini (The Netherlands)
- Rachel Splinters, Capgemini (The Netherlands)
- Fokko Dijksterhuis, Capgemini (The Netherlands)
- Richard B Harris, MITRE (USA)
- Kerry-Ann Barret, Organization of American States (OAS),
- Mark T Kajicek, SEI (USA)
- Vilius Benetis, GFCE Working Group B CIM TF Lead (NRD CS)
- Marc Henauer, GFCE Working Group B CIP TF Lead (Switzerland)
- Klée Aiken, GFCE Working Group B Chair (FIRST)
- Manuel Precioso Ruiz, GFCE Secretariat.

In case of any questions, please contact the GFCE Secretariat at contact@thegfce.org

Disclaimer

Table of Contents

Introduction to the guide

This publication seeks to provide guidance in designing, developing and evaluating how and when to conduct a tabletop exercise as a tool to improve an organization's cyber security policymaking and operations capacities. As indicated in the graphic below, this document is the first of a series of deliverables that will assist practitioners in identifying areas that would benefit from TTXs, as well as designing and implementing them in a way that increases cyber security capabilities.

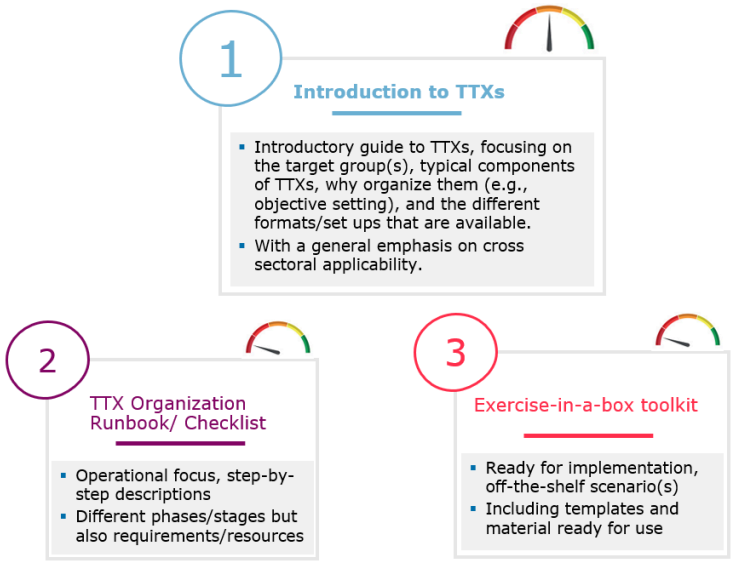
This guidebook is mainly aimed for:

- Cyber policymakers in governments,
- Cyber security preparedness and response organizations,
- Critical infrastructure owners and operators,
- Governmental and ministerial institutions (e.g., NCSCs) focused on implementing, national cyber security programs via policy or regulation,
- Technical community and other cyber security practitioners.

The guide aims to offer a public-private cross organizational scope. Therefore, this guide is not written from a strictly business point of view, but rather provides a macro-level approach to achieving cybersecurity resilience through TTXs. This way, organizations ranging from those which are part of critical infrastructure to others such as SMEs can make use and benefit from this guidebook.

The overall goal of the guide is to provide practical considerations to bridge the gap between technical operations and administration/politics in understanding the benefits of undertaking TTXs at all national and organizational levels and increase the knowledge of the personnel responsible for organizing TTXs so that they achieve their capacity building objectives.

This guide is part 1 of a three-deliverable package:



1. Introduction to table-top exercises (TTXs)

This chapter discusses the definition of a tabletop exercise (TTX) and why it is important to develop and perform a tabletop exercise. This is accompanied by an explanation of the potential goals of TTXs and the likely target groups for tabletop exercises.

Note: These are not all-inclusive exercise goals or potential target groups. Over time, scoping may differ due to rapid technological and socio-political developments, which will bring new needs and components into the cyber sphere. This will require a reflection into existing capabilities and may lead to additional characteristics into TTXs features.

What is a TTX?

A tabletop exercise is a scenario or simulation where personnel with roles and responsibilities in a particular Information Technology (IT) & Operational Technology (OT) plan and meet in various settings (e.g. breakout groups, virtually, in operation centers, etc.). Through these simulation exercises, organizations and individuals seek to test, discuss, rehearse and validate the content and functioning of an incident response plan, policies, responsibilities, procedures and to identify risks and draw lessons from it.

However, TTXs should also be valuable for their flexibility, allowing to not only test those aspects directly related to incident response plans but also useful for their ability to assess other needs and operations such as overall (threat) information sharing processes or policies, attribution, internal working structures, risk assessments, etc. For this reason, different customized variations are to be expected depending on an organization's size, needs and degree of investment[1].

Based on these variables and conditions, a facilitator will initiate the discussion by presenting a scenario and asking questions based on the scenario[2]. In timed exercises, ideally half day or 2–4-hour exercises, team members practice responding to a variety of threat scenarios in a setting that mimics the constraints of a real crisis.

TTXs bring key stakeholders together to work through a scenario for the purpose of testing pre-planned actions or adapting to unplanned scenarios. This format facilitates a holistic view of strategies and tactics, and allows participants to assess sufficiency and effectiveness, identify gaps, and suggest improvements.[3]

The purpose of a TTX is multifaceted, but the overarching intentions, which will be described later on this guide, are to enhance cyber capacity building and policy in a secure environment, through a cross-sectoral cooperative setting allowing the exchange of knowledge to facilitate cyber security resilience whilst respecting international norms.

[1] PWC. "Tabletop exercise". https://www.pwc.com/gx/en/issues/crisis-solutions/tabletop-exercises.html
[2] NIST. "Tabletop exercise". https://csrc.nist.gov/glossary/term/tabletop_exercise#:~:text=Definition(s)%3A,to%20a%20particular%20emergency%20situation.
[3] NARUC. "Cybersecurity TTX Guide". https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

Why conduct a TTX?

A TTX provides opportunities for participants to demonstrate and assess capabilities in specific areas of interest, including cyber risk management. They can also help to facilitate coordination and help clarify organizational roles and responsibilities.

Through TTX's one can improve overall cyber resilience to cyber threats by finding potential organizational gaps and enhancing security protocols whilst accelerating communication time. The operational landscape has rapidly changed over the years, introducing many new risks and uncertain technological developments, therefore cybersecurity organisations must adapt to these changes. TTXs are thus effective tools to discover and test adaptation capacities.

Emerging cyber threats have increased cybercrime vastly in the public and private sectors, especially since the pandemic began. Hackers and scammers use any possible resource available, from classic email phishing scams to AI/machine learning and other sophisticated technologies to steal sensitive information and hold organizations hostage.

Remote work further heightened the number of threats. While working from home allowed organizations to keep operating as usual, it also opened the door to new forms of cyber-criminal activity. Whilst people are returning to the office, as of today, there are more cybersecurity risks than ever before. Attacks have been of diverse nature and various means, however Ransomware as a service has stood out the most over the past years. The number of attacks has drastically increased, leaving organizations with the dilemma of paying the ransom, wiping their files, or attempting to improve cyber resilience through various means such as trainings and exercises.

The proliferation of asymmetric cyberattack has increased states and organizations use of ICTs, which necessitates the development of an international code of cyber conduct[4]. There is an urgent need for cooperation among states to mitigate threats such as cybercrime, cyberattacks on critical infrastructure, electronic espionage, and bulk data interception in cyberspace. All of these emerging threats could precipitate massive economic and societal damage and international efforts.

Types of threat actors can range from the following:

Threat Actor	Motivation
State Sponsored actor (APT)	Geopolitical
Cybercrime actors	Profit
Hacker for hire actors	Profit / Satisfaction
Hacktivist	Ideological
Insider Threat	Profit / Satisfaction

Tailoring exercises based on certain threat actors and cyber threats, which have the highest likelihood of perpetrating an organization, can help you to further assess potential risks and how to best mitigate them with the overarching goal of improving cyber security resilience. This should be in line with your organizational objectives/goals when it comes to assessing

[4] CFR. "Increasing international cooperation in Cybersecurity and Adapting Cyber Norms". https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

which areas you would like to test and improve as well as the overall risk that your sector is exposed to.

Learning Objectives

The identified learning objectives from the TTXs processes outlined in this guide are:

Individual participating organization:

- Testing communication and escalation lines/procedures within an organization. From technical/operational functions to strategic, management-oriented decision making.
- Reporting process in relation to policy when an incident occurs (e.g., NIS Directive, international law).
- Knowing when to trigger the legislation directive for organizations that are part of critical infrastructure.
- Testing organizational outreach to external stakeholders (e.g., how to handle media pressure, delivering press statements, communicating to partners/customers, public outreach).
    - At a macro-level, the scope is multifaceted: national vs regional, global coordination or at all levels.
- Discussing real life dilemmas. For instance, discussing a nation's incident response capacity & activation (NCSIRT), paying or not paying a ransom.

Cross organizational:

- Testing cross sectorial communication among numerous organizations (e.g., public/private).
- Testing cross organizational incident response capabilities.
- Testing cross organizational cooperation and resources in terms of capacity building.
- Testing cross-organizational channels to collectively mitigate real life cyber security threats.

Key benefits of TTXs more generally include the following:[5]

Team Building:

- Enhance training through practice.
- Create a stronger bond and willingness to work towards a common goal.
- Provide a needed outlet for problem solving and conflict resolution.
- Encourage employee collaboration and increasing cross-team communication.
- Foster new-found appreciation of others' strengths and weaknesses.
- Improve organizational and individual outlooks and attitudes towards preparedness.

Process development and refinement:

- Test and validate IR/Emergency response and Crisis Management plans.
- Ameliorate communication and reaction times.
- Validate escalation/reporting procedures.
- Clarify roles and responsibilities before, during, and after an incident.
- Fulfil compliance requirements and other due diligence.
- Examine plans, processes, and procedures for relevance and gaps.

[5] NARUC. "Cybersecurity TTX Guide". https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

Gap analysis:

- Identify potential (new) risks.
- Identify organizational challenges to a certain threat.
- Identify improvement points.
- Generate new ideas to solve knotty problems.
- Improve the organization's security posture by filling in the missing gaps.
- Identify resource constraints to meet risk mitigation goals and incident response objectives.
- Challenge the status quo.

Awareness:

- Improve overall cyber security resilience.
- Enhance awareness on cyber security challenges and responsibilities of an organization and the international community to address such challenges.
- Create a knowledge hub of information exchange among the cyber community.
- Undertaking Subject Matter Experts (SMEs) and technical experts for training and sharing knowledge regarding the matter.

Technology integration:

- Assess the compatibility of communication protocols and technologies.
- Assess the efficiency of the tools and mechanisms in place.

Cooperation:

- Assess cross-sectorial communication and stakeholder management.
- Help to develop cooperative solutions and initiatives to effectively address cyber security threats.
- Help to develop the appropriate mechanisms for cooperation amongst cross-sectorial organizations (e.g., critical infrastructure, government, private sector, NGOs).

Compliance with UN Norms for Responsible State Behaviour in Cyberspace:

From an ethical and international perspective, organizational objectives should be aligned with the United Nation's 11 Norms of responsible state behaviour in cyberspace. They reflect the common behavioural expectations that the broader international community has of each state and regional organization when interacting in the digital space. To state a few, the UN Norms aim to: promote interstate cooperation on security, protect critical infrastructure, ensure supply chain security and respect human rights & privacy[6].

Therefore, TTXs can add value to the implementation of these Norms by:

- Promoting broader collaboration through their common ground for cyber diplomacy.
- Serving as one of the pillars and main practices for the continuous reinforcement and learning processes on incident response (testing and assessing continuity and contingency), they ensure and encourage better compliance with UN Cyber Norms, particularly those directly connected to critical infrastructure protection across all stakeholders.

[6] UN Norms on Cyber Space. https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

- Enhancing awareness of the importance of better understanding and examining in greater detail how existing law is applied and implemented in the digital space.[7]

How to define the purpose and scope of your TTX?

Defining the overall purpose and scope of a TTX prior to developing or choosing a scenario is key, as the outcomes may differ. Therefore, you should assess what it is that you would like to test as well as what you envision to be the outcome of such an exercise. Having a clear understanding of what sort of achievements you would like to accomplish will facilitate the evaluation process, as well as its implementation to improve overall cyber resilience.

Some examples of other objectives that may drive scenario development are:

- Enhancing cross sectorial communication lines (e.g., reaction time, outreach, resources, collaboration, cyber diplomacy).
- Improving awareness within the organization of potential risks and challenges.
- Finding resource gaps whereby organizations can further invest in to ameliorate potential cyber security weaknesses.
- Improving compliance and due diligence in relation to reporting lines when an incident occurs within an organization.
- TTX could be used as a means to identify risks and potentially as a part of a broader risk assessment.
- A TTX could also be used to find gaps in organizations' cyber security measures. An exercise could serve as a means of conducting a maturity assessment within a wider scope of improving cyber resilience.

It is also critical to determine the exact scope of the exercise. Therefore, who do you envision as your target audience? What exactly do you want to figure out and test? Hence, you should look at the following to best determine your overall needs:

- Specific—addressing concrete questions, specifying action items and what sort of participants you would like to involve.
- Measurable—establishing metrics for success up front.
- Achievable by the participants in the time allocated.
- Relevant to the mission of the organization.
- Time-bound within a reasonable timeframe established in advance.

The exercise strategy particularly makes it possible to[8]:

- Raise awareness about cyber issues among staff and train those who have a role to play.
- Test and improve the efficiency of the procedures implemented under this scheme.
- Report on the efforts made in terms of cyber resilience and therefore meet any legal requirements and societal expectations.

[7] Switzerland FDFA. "Eleven Norms of responsible state behaviour in cyberspace", https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html

[8] ANNSI. "Organising a cyber crisis management Exercise". https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-organising_a_cyber_crisis_management_exercise-v1.0.pdf

Importance of implementing a holistic scope to exercises

It has already been stated that the TTXs should be geared towards a specific target audience with a specific output. With that said, it is important to also understand that the TTXs may look different as a result. The following options, in line with ENISA's good practice guide, outline an overview of the different approaches that can be taken when scoping the exercises.

Exercises inside an organization

Exercises are particularly useful for training staff on procedures to follow in the event of a cyber security incident at some point in the future. Therefore, they form an integral part of many organizations' business continuity planning as they provide crucial benefits:[9]

- Exercises ensure that staff are fully prepared and capable of responding to incidents by efficiently following business continuity and disaster recovery procedures.
- Exercises can reveal weaknesses in those procedures, such as unexpected implications of a type of incident, enabling managers to revise and improve procedures.

Interdependent Organizations

Most exercises are conducted internally by an organization, to test preparedness for potential disruptions, attacks or other emergencies. However, many incidents affect more than one organization.

- Attacks to critical infrastructure – e.g., telecoms, energy, water, emergency services, ministries.

Cooperative response

- Many incidents will require more than one organization to work together to solve the problem.
- Exercises can be a good means to test cooperation capabilities, resources, and capacity building.
- The ASEAN Cyber Security Exercise (TTX) implemented in 2019 Manila is a good example of various organizations and countries getting together with the goal of establishing common efforts and initiatives through ADMM-Plus[10].

Sectorial Exercises

Exercises can be held across a sector or multiple sectors. By training together, the participating organizations can achieve many benefits, such as:[11]

- Identifying interdependencies that they may not be aware of.
- Practicing working together with their counterparts at other organizations.
- Sharing best practices in their procedures.

[9] ENISA. "Good practice guide on national exercises". https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide
[10] ASEAN. "Development on ICT's Security @ADMM+Plus EWG on Cyber Security". https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-10-ADMM-PLUS-EWG-ON-CYBERSECURITY-PRESENTATION-1st-ISM-on-ICTs.pdf
[11] ENISA. "Good practice guide on national exercises". https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide

- Testing emergency contact information and channels of communication across organizations.
- Developing trust across organizations to jointly work together towards more resilient networks.
- Improving and demonstrating preparedness across partners, regulators, and customers.

Importance of recurring exercises

Benefits to authorities

TTXs yield other benefits for the public authorities for resilience within their area of expertise, be it communications, critical infrastructure, governmental etc. Authorities do not always have a high visibility of how individual organizations and their infrastructure will cope with an emergency. Therefore, conducting exercises can further help to:

- Determine how resilient organizations are.
- Identify weaknesses.
- Target action plans for improvement & measuring improvements.
- Target additional scenarios that organizations deem important (e.g., developing recurring exercise security roadmaps), or specific procedures/functions that may need improvement.
- Stimulate cooperation and public-private partnership in the efforts to increase cyber security resilience and capacity building.

Making TTXs a habit

Taking into account the overall benefits, this guide aims to further raise awareness and guide organizations to create a security/strategic roadmap of TTXs. This means that organizations should aim at having a series of exercises within the scope.

For instance, this would entail organizing 2-3 exercises per year testing various organizational aspects, from more technical/operational dilemmas, to strategic, external relations, auditing and compliance etc. Having such a roadmap in place will help organizations to improve overall cyber security resilience.

As a means of apprehending and summarizing the key takeaways and determining potential exercises down the road, it is crucial to conduct evaluations and lessons learned reports. After-action reports and brainstorming sessions on the exercise itself are critical aspects for improving an organization's security posture and readiness to face security incidents. Reporting helps to evaluate an incident's response performance, determines whether the exercise objectives were met and it can help to identify challenges and improve response capabilities going forward. The results and reflections of such reports can also serve as a hub of knowledge exchange within the international cyber community.

2. Scenario & set-up

This chapter describes how to set up a scenario that will be run through during a tabletop exercise. In addition, the design of a tabletop exercise is briefly discussed, with this design being discussed in more detail in future work in combination with a checklist of what is needed to make a tabletop exercise successful.

A tabletop exercise can be designed and developed in different formats and amounts of tailoring (e.g., lightweight or more complex TTXs). It is intended that organizational needs are identified and that the overall objectives, as described above, are highlighted. It must be clear in advance what needs to be tested and improved. In combination with the identification of the target group, it becomes clear what tabletop exercise is suitable and what the design options are.

Objectives

As discussed above, based on the organization needs, via various general objectives it becomes clear what subject(s) have to be included in the tabletop exercise. Identifying your organization needs consists in noting each problem, goal, or scenario, and the related progression of actions required to resolve it. Each subject can lead to a different kind of exercise or scenario. This means that before designing the tabletop exercise, it is needed to identify the objectives and subject needs of the organization.

These topics may vary, examples include:

- Data and information (internal/external data).
- Systems (IT, workflow etc.).
- Applications.
- Infrastructure.
- Processes.
- Client/customer relations.
- Communication (internal/external/cross sectoral).
- Response strategies / mitigation actions.

Sector/Target Groups

In order to decide what kind of tabletop exercise is needed, not only the objectives of the organization are of importance. It is also important to identify the target groups and/or sector beforehand. This TTX guide focuses on the cross-sectorial organizations. The target group is based on what groups and organizations would expect to be involved during a cyber incident. The different target and sector groups that can be applicable are the following:

- Governmental
    - State Officials
    - Policy Makers
    - Federal partners
    - Local government officials

- Critical Infrastructure: Utility owners/operations, energy sector, telecom, hydrology
- Non-Governmental Organizations
    - E.g., Red Cross

The exercise should include the most relevant stakeholders to participate in the exercise. This means that there needs to be made a clear selection that fits the objectives and needs of the organization.

Design

A tabletop exercise is being designed based on the applicable needs and objectives. As aforementioned, the design of a tabletop exercise can therefore vary. A menu card style method can be a beneficial approach to deciding the scalability of the exercise. The level of effort in building a scenario and implementing the TTX should be consistent with the overall objective and the resources available. Hence, TTXs can range from lightweight to more complex exercises.

More details about this topic will be included in the upcoming second deliverable of this project, the “Scenario Runbook/Checklist”. In this section, there will be a short introduction into the design requirements like format, scenario development, set-up and facilities.

Format

A tabletop exercise can make use of different formats. This is determined by the objectives and the target group. First, the format deals with the way of practice. This can take various forms. An exercise can take the form of a discussion regarding the most important dilemmas but can also be a full fletched exercise in which the network infrastructure of an organization is simulated. The following types of exercise can count as a tabletop exercise.

- Dilemma sessions
- Walk Through sessions
- Cyber Crisis Exercises
- Cyber Crisis Simulations
- Cyber Range exercises
  (Not within the original scope of a TTX. Can be seen as a potential next step or additional feature to a TTX).

In addition to the fact that the format of the exercise can differ in intensity, the format of the exercise can also be based on a certain type of exercise or phase of a cyber incident. A distinction is made between the critical phases at the time of a cyber incident, but also the phase after a cyber incident.

Exercises could for instance be on:

1. Incident response tabletop exercises
    - Making sure participants know what their organizations policies, depending on the type of attack, and who’s responsible for what actions in response to them.
2. Crisis Management tabletop exercises
    - Testing escalation procedures.

- Testing whether the right teams are in place and how to best facilitate cooperation.
- Talking to the right people at the right time.
- Coming up with strategic/operational mitigation actions.
- Downscaling accordingly.

3. Business continuity tabletop exercises
    - Resuming business operations and returning to regular day to day activities as quickly as possible.
4. Understanding your dependences on specific vendors/partners/operations and looping each one accordingly into any damage control scenarios for. Disaster Recovery tabletop exercise
    - Likely include the roles and responsibilities of personnel with regard to the processes and procedures associated with restoring an organization's information systems
5. Stakeholder management tabletop exercises
    - Organize scenarios based on internal and/or external stakeholder outreach.
6. Auditing/Compliance awareness
    - Testing reporting lines when an incident occurs (e.g., WBNI for CISA organizations).
    - Involving the relevant authorities when need be. Knowing when to escalate and how to report in due time.

It is important to mention that the above-mentioned formats of exercises can both take place physically and virtually. Being physically in a room for the exercise creates a good focus. It ensures that the participants can dive into the exercise without too much distraction, and they can directly consult and collaborate with each other. However, in times when organizations are working in a hybrid way, it is realistic that not everyone is at the same location at the time of a cyber incident. In addition, a cyber incident is not geographically tied to one place and can spread more quickly. This also makes a virtual exercise valuable.

Scenario development

A tabletop exercise uses a realistic, but fictitious scenario regarding a specific cyber incident. Depending on the target group, sector and objectives of the organization, different scenarios could be applicable. More information on the scenario development is described in the upcoming second deliverable of this project, the "Scenario Runbook/Checklist.

Types of potential scenarios:

- Ransomware attack CIIP**
- DoS
- Insider threats
- OT infra breach
- Third party software compromise
- BYOD
- Home & remote working
- Managing a vulnerability disclosure

A good example of how to define a scenario is the following: as soon as an organization has a runbook in place for ransomware (as an example), it is important to test this plan and the

operations of the organization. A tabletop exercise can be of added value here. Firstly, by going through the scenario with key stakeholders, it becomes clear where the missing gaps are. After improvements of the runbook, a complete cyber crisis exercise can be developed and facilitated, in which a scenario is discussed in more detail. This gives insights into the way of working of the participants.

Set-up

In a tabletop exercise, participants are expected to walk through a scenario and use any existing plans or procedures to respond appropriately. To ensure that an exercise runs smoothly, facilitators are present to guide the participants through the scenario. By means of injects, participants receive certain information about the scenario, which shows that a cyber incident is increasingly escalating. These injects encourage the participants to make action points and to clarify the decisions they have to make. During the exercise, the participants will be observed and evaluated. At the end of the exercise, the participants are given the opportunity to share experiences in a hot wash, after which the facilitators can initiate a structured discussion based on certain evaluation points. An exercise can then be concluded with the preparation of a report-out in which the most important evaluation points are identified and recommendations are given.

Facilities and requirements

In addition to the substantive preparation and set-up, it is also important to clearly map out the facilitation of the exercise in advance. This is because elements are identified that make it clear whether an exercise can be performed successfully.

It is important to make a clear plan for the preparation, execution, and evaluation of the exercise. This may depend on the size and complexity of the exercise, preference, degree of commitment by participants, and the amount of resources dedicated to it. In addition, it is important to make clear agreements in advance for the use of any tooling during the exercise, for example about the way of communicating.

3. Conclusion

This document discusses the importance of developing and executing TTX exercises regarding critical infrastructure. It emphasizes what the goals of such an exercise can be, which target groups are important when looking at cross-sectorial collaboration and what the components are to set up such an exercise. Future work elaborates on the design of an exercise and explains use cases, identification of best practices and example scenarios.

As a follow up to this “Intro to TTXs” deliverable, the following two deliverables, 2) “TTX Runbook/Checklist”, and 3) “Exercise in a box toolkit”, will provide detailed information on how to organize and execute a TTX. Whilst this guide provides a good basis and overarching approach to what, who, how and why TTXs are essential for improving cyber resilience, the following two deliverables focus more on the operational context.

Deliverable two serves as more of a step-by-step description focusing on the different phases and requirements/resources needed to prepare and execute a TTX, whilst deliverable 3 will provide a ready for implementation off the shelf scenario to test out the processes.

Overall, the three deliverables are part of a unified package, going hand in hand, to help organizations conduct and benefit from TTXs effectively.

4. References

- ANNSI. “Organising a cyber crisis management Exercise”. https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide--organising_a_cyber_crisis_management_exercise-v1.0.pdf

- ASEAN. “Development on ICT’s Security @ADMM+Plus EWG on Cyber Security”. https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ANNEX-10-ADMM-PLUS-EWG-ON-CYBERSECURITY-PRESENTATION-1st-ISM-on-ICTs.pdf

- ASPI. “UN Norms of Responsible State Behaviour in Cyberspace”. https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

- CFR. “Increasing international cooperation in Cybersecurity and Adapting Cyber Norms”. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

- ENISA. “Good practice guide on national exercises”. https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide

- NARUC. “Cybersecurity TTX Guide”. https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

- NIST. “Tabletop exercise”. https://csrc.nist.gov/glossary/term/tabletop_exercise#:~:text=Definition(s)%3A,to%20a%20particular%20emergency%20situation.

- PWC. “Tabletop exercise”. https://www.pwc.com/gx/en/issues/crisis-solutions/tabletop-exercises.html

-Switzerland FDFA. “Eleven Norms of responsible state behaviour in cyberspace”, https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html