CSS CYBER DEFENSE REPORT

Cybersecurity and Cyberdefense Exercises

Zürich, September 2018

Cyber Defense Project (CDP)
Center for Security Studies (CSS),
ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Dr. Robert S. Dewar

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Please cite as: Robert S. Dewar (2018): Cyber Defense Report: Cyber Security and Cyber Defense Exercises, September 2018, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

1	**Introduction**	**3**
1.1	Context and Goal of the Report	3
1.2	Summary of Findings/Lessons Learned	4
1.3	Terminology to be used in this Report	4
1.4	Overview of the Report	4
1.5	Methodology for the Report	5
1.6	Disclaimer	5
2	**Background to the Study**	**6**
2.1	Why are Exercises important?	6
2.2	Exercises as teaching tools: Active Learning	7
2.3	What exercises are currently being carried out?	7
2.4	Previous studies of Cyber Security and Defense Exercises	8
3	**Goals: Why Conduct Cyber Exercises?**	**10**
3.1	Identification	10
3.2.	Testing mechanisms and/or procedures	11
3.3.	Exercising mechanisms and/or procedures	12
3.4.	Increasing communication and co-operation	12
3.5.	Developing policy	13
3.6.	Exercise audiences	14
4	**Types of Exercises**	**15**
4.1	Full Simulation or Table-top Exercise?	15
4.2	Specific types of exercise	16
4.3	Considerations when selecting an exercise type	17
5	**Resources**	**18**
5.1	The “Basics” of organizing events	18
5.2	An effective, well-resourced supporting infrastructure is needed	18
5.3	Adequate resources are crucial	20
6	**Actors/Participants**	**21**
6.1	Who participates is highly dependent on the goals of the event	21
6.2	The “usual suspects” of simulated cyber events	21
6.3	Goal-Actor interdependencies when organizing events	22
6.4	Relationship with the media	22
6.5	The challenge is which participants to invite	23
7	**Conclusions and Lessons Learned**	**24**
7.1	Context is crucial	24
7.2	Planning is key	25
7.3	Have realistic scenarios	26
7.4	Cyber ranges not called for	26
7.5	Don’t conduct exercises simply for the sake of conducting exercises	26
8	**Bibliography**	**27**
9	**Appendices**	**29**
9.1	List of acronyms and abbreviations used	29
9.2.	List of exercises examined	30
9.3.	Useful publications relating to the conduct of exercises	33

1 Introduction

1.1 Context and Goal of the Report

The nature of global security challenges has changed dramatically in recent years. From large-scale acts of international terrorism to ongoing civil war spilling over into neighboring countries, the security landscape is fluid. One of the most prominent security concerns has been the rise in the use of digital tools and to conduct malicious and damaging cyber incidents. These incidents range from high-profile, sophisticated tools targeting specific hardware (such as the discovery of Stuxnet in 2010) to the exfiltration of data from military contractors, such as that experienced by the Swiss military equipment manufacturer RUAG (Jürgensen, 2017; RUAG, 2016). In the Swiss context, cyber security and cyber defense are now important policy considerations at the cantonal, national and international level. Policy-makers around the world are seeking out ever more creative policy frameworks to respond to and mitigate cyber incidents.

One of the key questions facing policy-makers is how best to prepare for a cyber incident: which resources, tools, expertise and systems are required to either prevent an incident occurring or to minimize the impact of an incident should it occur? A useful and productive method for identifying these elements is by conducting exercises – simulated and controlled replication, observation and discussion of cyber security incidents. Such activities not only test levels of national or regional preparedness, but can also identify gaps and areas for improvement. The types of exercises conducted range from full simulations and replications of cyber-incidents and cyber-induced failures of critical infrastructures to one-day, policy-centered discussion events or workshops following a BOGSAT[1] format. Conducting cyber exercises – whether large-scale simulations or small-scale workshops – is therefore an important and useful way to ensure that defenders are prepared should a cyber incident occur. One tool for achieving this preparedness is through the use of what are known as "active learning techniques". Active learning is a pedagogical technique designed to improve students' and participants' absorption of lesson content, theories and concepts. It is an approach that shifts learning away from passive, instructor-focused teaching via lectures and seminars to more student-focused approach prioritizing learning interactive experiences (Krain and Shadle, 2006, p. 52). The use of scenarios and simulations where students and participants are required to apply specific techniques in a controlled environment can provide those participants with a deeper understanding of the constraints, resources and political processes required in a given situation, such as a cyber-incident. Therefore, by definition, cyber exercises such as *Cyber Europe* or *Locked Shields* are active learning tools.

The number of cyber exercises has increased over the last 10 years. A study conducted by the European Network and Information Security Agency (ENISA) identified three reasons for this increase (2015, pp. 26–28). The first is that an increase in the publication of national and international policy and strategy documents supporting the staging of such exercises. This increase in policy publication has come about as a response to an increase in the occurrence of real-life incidents and increased attention paid to cyber incidents in the public imagination. Governments and international organizations wish to be seen to be responding to the rising number of cyber security breaches and cyber-incidents and reassure an increasingly-informed public.

The second reason for the increase in the number of exercises is that these exercises are responses to "wake-up calls": an increasing number of publically acknowledged incidents and reports on incident that are raising awareness of cyber security issues. These incidents are increasing in complexity, highlighting changes in the threat landscape and necessitating national and international preparedness initiatives, of which exercise are a part. As a result potential large-sale cyber incidents have become associated with other forms of crisis management such as natural disaster response. This a field in which exercises and simulations have long played a role in preparation.

Finally, ENISA has recognized that "exercises generate exercises". Large scale events such as the *Locked Shields* (hosted by the NATO Co-operative Cyber Defense Center of Excellence) or ENISA's own *Cyber Europe* exercises have a snowball effect, with participants and observers acknowledging the benefits of these activities and seeking to host their own forms of simulations, scenario-based discussions and workshops.

The purpose of this Report is to detail the utility of exercises in the context of cyber. It examines the goals of cyber exercises, what types of exercises are available for practitioners, which actors take part in exercises and why, and which resources are needed to stage a successful exercise. The benefit of exercises and drills in military and security circles, as well as the benefits of cyber-specific exercises, have been stated previously. However, what precisely those benefits are has to date not been examined. This Report will not only provide an insight into the practical benefit conducting exercises can bring to cyber security and cyber defense policies and strategies, but will also provide insights into the lessons learned from previous exercises.

[1] BOGSAT – Bunch Of Guys Sat Around a Table

1.2 Summary of Findings/Lessons Learned

There were six core findings in the research conducted for this Report. The most significant is the importance of **context**, specifically the context of the goals exercise organizers seek to achieve. All decisions relating to the nature of the exercise – whether it is a full simulation or table-top activity, the resources required, which participant demographics to include – are all derived from the goals of the exercise.

As important as context is adequate **planning** prior to staging an exercise. Problems of resource allocation and decision-making can be addressed with sufficient planning and lead-up. This is highly relevant to the third finding, that **adequate resources** are vital to the success of an exercise. While relevant and appropriate resources – computers, software, venues, support staff, an effective maintenance infrastructure – are vital to that success, ensuring that there is *enough* of a resource has been a frequent point made in the after action reports of the exercises examined here.

An important element of the planning stage is to ensure that **scenarios are realistic**. Simulated cyber-incidents of a scale leading to widespread death and destruction, complete infrastructure failures, or military takeovers are "worst-case scenarios" but are unrealistic when it comes to cyber-crisis management. While such scenarios are not out-with the realms of possibility, no real-life cyber incidents have come close to this level, and so preparing for such situations would not be a prudent use of resources. This leads to the fifth finding: **bigger is not necessarily better**. Large-scale, multinational simulations have a place in active learning, but if the specific goals of an exercise can be achieved with a smaller, less resource-intensive BOGSAT exercise, then this is a more effective use of time and resources.

The final finding is more practical. The AARs and exercise reports studies here have **not recommended the establishment of dedicated cyber ranges**. Cyber ranges are specialist, secure networks and systems where offensive and defensive cyber tools can be tested in much the same way as testing ranges for conventional weapons. Those that have been constructed are used by both private sector entities working in the field of cyber defense and security and national security entities to develop and test capabilities. Such facilities would appear to be a logical environment in which to conduct cyber exercises, especially if there is a technical component to such activities. From an active learning perspective, having a specialist facility where actors can learn about and how to use specialist capabilities also makes good sense. Paradoxically however, in the research for this Report such cyber ranges were conspicuous by their absence. Despite have an important part to play in the testing of digital tools, from a preparedness and crisis management perspective cyber ranges are not a priority.

1.3 Terminology to be used in this Report

Accurate and consistent terminology has long been a problem for cyber security and cyber defense studies (Dewar, 2014; Kruger, 2012). There are no internationally agreed definitions for terms used in policy and strategy documents. The same is true when examining cyber exercises. Terms such as "simulation", "scenario" and "exercise" often used interchangeably as well as referring to specific activities or aspects of activities. To avoid any confusion, this Report will adopt the International Organization for Standards terminology published in its Guidelines for Exercises (ISO, 2013). These guidelines describe exercises as "processes to train for, assess, practice, and improve performance in an organization". Exercises provide a controlled opportunity to validate policies, plans and procedures as well as train personnel in roles and responsibilities. As such, the word "exercise" will be used in this Report as a general term to cover all types of cyber security activity where an element of self-reflection and learning in a hypothetical situation takes place. This covers large-scale events featuring complex digital simulations as well as small table-top, paper-based workshops with no technical elements. This is to avoid confusions of nomenclature and maintain a focus on the activities themselves.

A final point to make on nomenclature and terminology relates to the word "drill". In military terminology, drills and exercises occasionally relate to similar activities, particularly when referring to training sessions. To avoid any confusion arising from the use of both "drill" and "exercise" to describe conceptually similar activities, this Report will adopt a stricter definition of "drill", where the term is used to describe systematic training in particular techniques or tools through multiple repetition. The repetitive, systematic nature of military drill is what differentiates it from other types of exercises.

1.4 Overview of the Report

Following this Introduction, Chapter 2 of the Report provides a background to the research and topic. The chapter sets out why exercises are important, with a particular focus on what it is cyber exercises can bring to policy development, strategic oversight, resource management and preparedness planning. The chapter also briefly explains the concept of active learning, looking at how and why exercises are beneficial teaching tools when seeking to defend against or mitigate cyber-incidents. This background chapter also provides a brief overview of current high-profile cyber exercises, but also highlight a number of smaller, national events that nevertheless provide useful findings and lessons learned.

Chapter 3 explores the goals of cyber security and cyber defense exercises: what are organizers and

participants trying to achieve? The chapter illustrates why clear goals are vital to the success of an exercise, to the extent that they underpin all other aspects of these activities.

Chapters 4, 5 and 6 examine the basics components of staging a successful exercise. Chapter 4 focuses on the various types of exercises that can be conducted and which factors should be considered when staging one. A focus is placed on how conducive these activities are for active learning. Chapter 5 examines the resources necessary to stage a successful exercise, focusing on the fact that, once a decision is made on the nature of resources, having adequate resources is crucial. Given the secrecy and classified nature of many government cyber security and defense capabilities precise figures are not provided. Instead the chapter focuses on which resources are useful, rather than quantities. Chapter 6 looks at participant demographics, examining which actors routinely take part in cyber exercises and acknowledging that participant demographic is highly contextualized, and dependent on the goals of the exercise itself. An important aspect of this consideration is maintaining a positive relationship with the media.

Finally, Chapter 7 summarizes the Report's findings and highlights key lessons learned.

1.5 Methodology for the Report

Research for this Report was carried out using desktop-based research methods. The first step was to collect relevant literature sources. This involved sourcing the After Action Reports (AARs) of a number of national and international exercises, and any industry or academic examinations of exercises. In total 14 AARs were examined, ranging from national to international exercises. A full list of is provided in Appendix 2 of this Report. The AARs were invaluable sources of information relating to the planning, implementation and lessons learned when staging exercises, while higher-level studies such as those produced by ENISA provided more insights into the similarities and comparisons of exercises already carried out. A substantial number of data sources was accumulated, yielding useful insights and information. These literature sources were complemented by industry-based sources, in particular from the disaster and crisis management sector and what information was available on cyber security exercises, particularly that published by ENISA.

Data for the Report was also gathered from a series of interviews with experts in the field. Interviewees were provided with questions in advance, which were used in semi-structured conversations conducted either by telephone or face-to-face via Skype. Interviewees were divided into those who *organized* exercises and those who *participated* in them. This was conducted to gain further practitioner and participant insights into the organization and conduct of cyber exercises. A number of interviews, however, were conducted with experts who had experience both as organizers and as participants, offering a unique view from both sides of an exercise. Interview responses were then fully transcribed.

All sources – literature-based and interview-based – were uploaded into MAXQDA data analysis software. Using qualitative data analysis software in this manner facilitated the analysis to identify trends, common lessons learned and techniques. A list of exercises examined and their concomitant AARs is provided in Appendix 2.

1.6 Disclaimer

The data for this Report was drawn from available open-source material which is of great value but also somewhat problematic. Many incidents, both in the private and public sector, go unreported due either to their classified targets or fear of reputational damage. The latter is particularly the case for multinational corporations not wanting to appear unable to adequately secure their assets or customer details. Similarly, a large number of cyber security and defense exercises are conducted as internal teaching tools, or remain classified. As a result, building a complete data set of cyber exercises is challenging. The exercises, scenarios and simulations used in this study were already in the public domain and are well documented in cybersecurity and defense literature. As a result, the data sets presented here are not completely representative, but nevertheless comprehensive enough to draw the conclusions presented in the Report.

2 Background to the Study

This chapter sets out the rationale for conducting the research for this Report by exploring why cyber exercises are useful tools for security practitioners and policy makers. There are four aspects to this rationale. First, the chapter will first set out why exercises are important tools in a general context, and not specifically related to cyber security. As activities, exercises can bring together numerous organizations and entities necessary for a particular goal – such as ensuring national cyber security – and facilitate communication between those entities.

Secondly, exercises are useful teaching tools and the chapter will set out *why* this is the case: what is it about exercises that makes them such good training tools? An answer to this question is found in the concept of active learning, where teaching and training is not carried out through lectures, but instead focusses on ensuring students and participants use their knowledge in interactive ways such as simulations or scenarios.

In the third section the chapter will briefly set out which exercises are currently being carried out, exercises which will form the core data sources for the research. There is a significant number of international cyber exercises being conducted, both in the US and in Europe, which bring together actors and entities from across the cyber security spectrum. These include military and security actors, private corporations and government ministries.

The final section of the chapter also positions the Report in the wider research on cyber exercises. The European Network and Information Security Agency (ENISA) has conducted a number of studies of cyber exercises which include details on the kinds of activities which comprise those exercises. This Report will build on those findings by providing a more nuanced analysis by re-orienting the analysis towards a focus on goals and objectives.

2.1 Why are Exercises important?

The advantages of using exercises such as simulations as training tools have been well known to military and security personnel for centuries (Weitz, 1998). In the 4th century the Roman military strategist Vegetius wrote that new recruits needed to drill effectively as "drill-at-arms" was the only explanation for "the conquest of the world by the Roman People" (Vegetius, 2001, p. 2). Also in the context of training and military strategy, games and simulations were well known to Roman military commanders as tools to visualize and manipulate small physical representations of battlefields (Smith, 2010, p. 7). Such activities provided practice for soldiers in preparation for real situations and actual combat. Using exercises to defend against and mitigate cyber-incidents reflects the application of long-standing and effective techniques against the latest security threats.

Exercises are also useful tools beyond pure training and drill. From the perspective of organizational learning, there is no fundamental difference between a simulated event and a real incident (Prior and Roth, 2016, p. 15). Conducting exercises can help with validating policies, plans and procedures, as well as with training, improving current tools or rolling out new equipment, testing information and communications technology (ICT) and identifying gaps in resources. In terms of policy development and preparedness, the International Organization for Standardization (ISO), in its Guidelines for Exercises stated that "exercises are an important management tool intended to identify gaps….relevancy and accuracy" (ISO, 2013). As a result, they are of benefit to a broader range of actors and organizers than simply military and security organizations. They can be carried out by small, individual entities such as single ministries or private firms or, in the case of large, multinational simulations, exercises can involve a multitude of actors from different areas of the security nexus, such as private corporations, government ministries, utility providers and military units (Department of Homeland Security, 2006, p. 15).

Exercises are invaluable tools for planning and identifying necessary equipment, techniques and processes in all manner of disaster and crisis management strategies (Australian Institute for Disaster Resilience, 2012) as well as promoting awareness of threats in the public and political domains and, perhaps most importantly, promoting awareness of solutions and contingencies to reassure those demographics. Exercises – be they full-scale simulations or simple table-top discussions – are therefore invaluable, multipurpose tools for situational awareness and incident preparedness, attributes vital to effective cyber security and cyber defense. As stated by Prior and Roth in the context of disaster training exercises (2016, p. 16), such activities provide "a controlled mechanism to test implemented organizational arrangements and procedures" to ensure that planned responses are as fit for purpose as possible.

A further advantage of using exercises to promote cyber security and defense is that they can be conducted at any scale commensurate to the needs of the organizers and exercise goals. As mentioned above, exercises can be small discussions taking place over one or two hours, with participants sitting around a table. At the other end of the spectrum are much larger multinational simulations, similar to the international naval or army exercises carried out by military allies and partners. These large cyber simulations replicate the circumstances of cyber incidents in a controlled environment, enabling participants to experience as real a situation as possible. This has the advantage of being

able to recreate complex, dynamic political processes in a controlled environment, enabling participants to "examine the motivations, behavioral constraints, resources and interactions among actors" (Smith and Boyer, 1996, p. 690). In the cyber context, therefore, exercises – large and small – can achieve specific objectives beneficial to cyber security and defense. For example, they bring together those entities, organizations, institutions and agencies with collective responsibility for cyber security at the local, national or international level in order to improve communication and information sharing. Exercises with shared goals go some way to ensuring that communications channels between these entities are open, can identify where such channels need to be created and allow for contingencies to be developed should communications channels be disrupted by a cyber incident.

2.2 Exercises as teaching tools: Active Learning

An important aspect of cyber exercises – indeed any exercises conducted by military, security or crisis management agencies – is the pedagogical value such activities provide. At one level, the answer to the question "Why conduct exercises?" is that they provide an opportunity to test resources, drill responders and identify areas for improvements to preparedness or clarify communications channels. To provide an effective and holistic analysis of exercises it is prudent to understand how and why these activities work so as to demonstrate their educational value.

The use of simulations and scenario-based activities as learning tools form a core part of what is known as "active learning". Active learning is a teaching tool which seeks to achieve more than can be done through lectures or learning by rote. Learning through interactive activities such as simulations and scenarios seeks to stimulate experiential learning (Krain and Shadle, 2006, p. 52). Rather than simply memorizing information, exercise participants utilize knowledge in practical situations. In other words, exercises encourage participants to use skills, techniques, tools and policy frameworks they know *in a practical, simulated environment* in order to be better prepared should a real crisis ensue. The key feature of active learning is that participants *apply* what they know in a controlled environment.

Simulations, games and role-play activities are core elements of active and participatory learning and can deepen participants' and observers' understanding of a particular phenomenon (such as a cyber-incident) by bringing previously unlived experiences, events and situations to life. Simulations and war-games can recreate complex processes, enabling the examination of actor motivations, behavioral constraints, resources and interactions in a given situation (Smith and Boyer, 1996, p. 690). Bringing these hypothetical situations to life in this manner, and enabling participants to actively engage with those situations, makes them better prepared to act if and when a situation occurs in real life.

Active learning as a concept is therefore a very powerful tool for military, security and crisis management actors and goes some way to explaining how and why exercises such as cyber simulations are so useful and important when establishing individual and organizational preparedness and resilience to cyber incidents. Cyber security and defense exercises provide opportunities for participants to apply theoretical, hypothetical concepts in a physical environment (Hoffman et al., 2005) without fear of adversely affecting the "real world". The techniques of active learning are therefore invaluable as they focus on participants' activities; maximize participation; are motivational and give immediacy to the subject matter, something of great benefit to a fast-moving, rapidly changing environment such as cyber security. For these reasons active learning will be referenced throughout this Report

2.3 What exercises are currently being carried out?

In addition to exercises, drills and scenarios having been used for training and awareness purposes for centuries, exercises have been used to bolster cyber security and defense for decades. Recently declassified material from the US describes Operation Eligible Receiver, a cyber defense exercise targeting critical infrastructures which was conducted in 1997 (Cyber Defense Magazine, 2018; Martelle, 2018). Since that time, the number of exercises being carried out at national and international level has increased exponentially. A report published by ENISA on national and international cyber security exercises found that there was a steady increase after 2000, with spikes in activity corresponding to the occurrence of important international cyber incidents, namely the Estonian DDoS incidents of 2007, the Russo-Georgian conflict of 2008 and the discovery of Stuxnet in 2010 (ENISA, 2015, p. 14).

Exercises are being carried out at all levels. Some of the most high-profile activities are large, multinational exercises simulating cyber-incidents targeting international critical infrastructures. These include the *Locked Shields* and *Baltic Shields* exercises conducted under the aegis of the NATO Co-operative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, and the *Cyber Europe* and *Cyber Atlantic* exercises conducted by ENISA. These exercises include a technical dimension, with participants using digital tools to mitigate and counter cyber incidents. There are also non-technical exercises such as the annual *Cyber 9/12 Challenge*. This is a desk-based activity inviting students from around the world to develop policy solutions to a particular unfolding scenario. As such the resources

required were limited to a venue large enough to host the number of competitors' groups.

These large-scale exercises are designed to encourage cooperation between entities and identify channels of cooperation that will facilitate cyber defense across the participant demographic, but also test readiness of individual entities in the face of a simulated cyber incident. These exercises tend to follow a traditional war-game pattern, with capture-the-flag activities or attacker/defender models to test the abilities of defenders to withstand concerted attacks in a controlled environment. As will be discussed in Chapters 4 and 5, these types of exercises are highly resource intensive, requiring a great deal of planning prior to the exercise but also an efficient maintenance infrastructure during the exercise execution.

There are also high-profile exercises conducted at the national level. The US government's *Cyber Storm* exercises are run regularly at (almost) bi-annual intervals. This is a very large-scale undertaking which routinely draws in over 100 participants from around the world and across the spectrum of entities involved in cyber security and defense (Department of Homeland Security, 2009, p. 1,19). At a smaller, more intense scale, the Czech Republic's national computer emergency response team (CERT) ran an exercise in 2016, the feedback presentation for which provided insights into the practicalities, lessons learned and networked infrastructure required to stage an exercise in a small but heavily connected state (Vykopal and Mokoš, 2016)[2]. These single-state activities also require significant resources, but are logistically less intensive. International, secure networks are not necessarily required, particularly if the actors involved are representatives of a government administration.

It is worth pointing out that active learning tools beneficial to cyber security and cyber defense need not be limited to crisis management or incident response scenarios. Andreas Haggman of Royal Holloway University of London has devised a board game – "The (Great) Cyber Game". This game is loosely based on the UK's National Cyber Security Strategy and creates an adversarial setting for players to engage with key cyber security concepts. This game is mentioned here for two reasons. First, it is targeted at practitioners, policy-makers, legislators and executives, in order to demonstrate the issues that are prevalent when seeking to understand cyber security from a conceptual perspective rather than a technical one. The objective is to step away even further from highly technical, device-based simulations and discussions and examine the political, practical and societal impacts of a cyber conflict (Haggman, 2018a). The second reason the game is mentioned at this point in this Report is to demonstrate the scope of activities which can be utilized as active learning tools. Cyber-specific games such as that devised by Haggman can be used today to understand past events, "plan operations and organizations and explore envisaged futures" (Haggman, 2018a) for cyber incidents in much the same way as table-top representations were used by Roman military commanders as tools to visualize battlefield maneuvers and marshal troops (Smith, 2010, p. 7). In the case of Haggman's game, gameplay allows players to see and understand the relationship between central government, businesses and society, and the impact a cyber incident can have on these three social sectors. Such games are therefore invaluable teaching tools.

2.4 Previous studies of Cyber Security and Defense Exercises

There have been previous studies conducted relating to the conduct and benefit of exercises, including guidelines on how to stage exercises[3]. The Center for Security Studies (CSS) at ETH Zurich published a study in 2016 examining how both real-life disasters and simulate exercises can be used as learning tools for civil protection organizations (Prior and Roth, 2016). The International Organization for Standardization (ISO) produced in 2013 a short, five-page document setting out a set of terms and definitions, as well as guidance for the planning and execution of exercises. Because the ISO guidelines were designed to be as generalizable as possible, they do not provide a great deal of detail or precise instructions. By contrast, one of the most comprehensive guides on the planning and execution of exercises was published a year earlier in 2012 by the Australian Institute of Disaster Resilience (2012). This document is a manual – a how-to guide – detailing what exercises are, why they should be conducted and how to plan and execute one. It provides invaluable details on exercise design, staffing requirements, documentation and resource management and provides a model for managing exercises. It must be pointed out, however, that this manual is targeted at those entities and individuals tasked with disaster management such as floods, fire and physical infrastructure failure. There is no mention of cyber security or digital infrastructure management. The ISO guidelines also do not make specific reference to cyber security exercises. Nevertheless, the guidance from both of these documents is very relevant for cyber security and defense exercises. A comparison of the guidelines provided in these documents with the steps taken by

[2] As stated in the Disclaimer in Chapter 1 of this Report, identifying national level exercises with findings, lessons learned or AARs in the public domain proved challenging. These results of national exercises often remain classified, particularly if there is heavy involvement from national defense ministries.

[3] A list of useful documents relating to exercises, including those used for this Report, is included in Appendix 9.3 of this Report

event organizers and published in exercise AARs shows the transferability of the ISO and Australian guidelines.

Current literature also shows that non-traditional entities are becoming involved in cyber security exercises, with a view to bolstering their own capabilities. Hoffman et al (2005) published a document in 2005 examining how a cyber exercise program, based around competitions, could be developed for universities. They cite the advantages such a program could bring for education purposes as well as enhancing security, and examine the resource requirements, scale and limitations of a number of exercise types. While this demographic does not often feature in literature covering cyber exercises, it is important and useful to note that many of the authors' recommendations match up with those of the ISO and Australian publications. Guidelines for cyber exercises, and exercises in general, are therefore multipurpose in the sense that they can be applied to numerous different operational areas to good effect.

While there are published guidelines on the conduct of exercises, reports on cyber security and cyber defense exercises in general are sparse. Due to its work organizing exercises for the European Union (EU), the European Network and Information Security Agency (ENISA) has conducted its own research into national and international cyber security exercises. Two reports published in 2012 and 2015 provide an overview of exercise types, resources needed and participant demographics. As such they provide a great deal of information pertaining to exercises in the European context, what kind of scenarios and simulations are used, and some detail regarding the objectives of the exercises. The reports also highlight the recognized need for communication between entities responsible for providing and ensuring cyber security and defense.

There are fewer details, however, on the interrelationship of these variables. As will be examined in Chapter 3 and the conclusion of this Report, successful cyber exercises are highly contextualized, and that context is provided by the goals of the exercise themselves. These goals – which must be clearly articulated during the planning phase of an exercise – to a large extent dictate the nature of the exercise, the resources required and the participant demographic. This is a level of detail and interrelation that is not immediately provided in the ENISA reports, or the other publications relating to cyber exercises published by the ISO or the Australian government. As a result, one of the additional goals and objectives of this Report is to contribute to this body of literature by examining that contextualization and providing a more nuanced examination of cyber exercises.

3 Goals: Why Conduct Cyber Exercises?

The study of exercise AARs and the interviews conducted identified a wide range of objectives and specific outcomes the organizers sought to achieve, as well as a range of objectives on the parts of the participants themselves.

These goals stated can be distilled into five broad categories, representing strategic objectives to be reached when staging an exercise. These goals are:

1. Identification
2. Testing mechanisms and/or Procedures
3. Conducting drills
4. Increasing communication and co-operation
5. Developing Policies and procedures

At first glance these goals correspond to those set out by the ISO (ISO, 2013). However, closer examination shows that the goals set out here are more idiosyncratic and relevant to cyber exercises. They have been drawn from the AARs and interviews conducted for the Report. These goals are presented in Table 1.

While there are other exercise-specific objectives (such as increased military co-operation for *Locked Shields* or better Member State co-ordination in *Cyber Europe*), the five goals set out in Table 1 and described here are present in in all the exercises examined. As such, these five represent core generic, but trending goals throughout the research. It would be prudent for exercise organizers to keep these five goals at the forefront of any exercise organization in order to maximize its effectiveness and ensure effective pre-event organization such as choice of activity[4].

3.1 Identification

Identification refers to several specific objectives. These range from the staging of simulated exercises leading to the identification of specific roles in the provision of cyber security that need to be filled (Murphy, 2017), to reviewing a flawed aspect of policy or procedure identified during a previous exercise or actual incident. The full range of identification actions established as goals for staging exercises can be collated into three trends or categories.

Table 1: Categories of Goals for Cyber Exercises

Goals	Description
Identification	Highlighting and identifying vulnerabilities, procedural flaws and information-sharing mechanisms
Testing mechanisms and/or procedures	Evaluation of already-established tools, practices and procedures to determine if these structures are fit for purpose or to find out if newly-developed practices and structures function as intended.
Drills	Using established mechanisms and/or procedures to ensure readiness in the event of an actual incident occurring, but also to avoid complacency of responders and atrophy of capabilities. Crucially, *exercising* mechanisms is considered to be different from *testing* those policies or techniques.
Increase Communication and Co-operation	Identifying or re-establishing channels of communication between actors, in particular actors with different real-world priorities, such as public and private sector entities or different national cybersecurity frameworks. Regardless of these differences, effective information-sharing is critical to successful response.
Developing Policies and Procedures	Developing and producing new and more efficient methods and response procedures where none existed prior to the simulated exercise. Testing and exercising mechanisms, including policies and procedures is contingent on those policies and procedures already in place. If an entity is engaging in a development process, then a simulated exercise can facilitate that development.

[4] See Chapter 4 on the nature of exercises

3.1.1. The identification of technical or systemic vulnerabilities in networks (also a facet of penetration testing)

A number of AARs and interviews cited identifying vulnerabilities as a core goal for staging an exercise. While this is one of the most obvious goals it is also one of the most important. In addition to testing the robustness of systems and networks (see point 2 below) and exercising established protocols for incident response (see point 3 below) staging cyber exercises can uncover hitherto unknown systemic and/or zero-day vulnerabilities. Such identification is a core component of Capture the Flag (CtF) exercises or traditional military war gaming (red-teaming). These exercises can be conducted on a range of exercise scales, from large-scale international exercises to small exercises conducted inside corporate or government networks.

3.1.2. The identification of policy, process or procedural issues that affect responses

These can be general or generic goals, such as identifying the gaps in responses to large scale cyber incidents (ENISA, 2012a, p. 4) or specific goals such as identifying areas for improvement in policies and procedures as a result of past exercises (Australian Institute for Disaster Resilience, 2012, p. 15). In both cases a goal is to identify any practices, policies, procedures or aspects of process that could hinder responses to or inadvertently assist an incident. As is the case with all simulations and war-games, conducting exercises in a controlled manner and environment – where malicious incidents are replicated but without the risk of actual infrastructure or systemic damage – can highlight these flaws and provide insights into what needs to be remedied to reduce the impact of a real incident.

One of the most important acts of identification does not relate specifically to cyber defense measures, however. The first relates to the legal parameters in which those measures are used. Staging a simulated exercise can help to identify legal or national policy bottlenecks which hinder the deployment of effective response tools (Department of Homeland Security, 2006). While it is important to identify which policies and legal frameworks are conducive to cyber defense, identifying those which prevent action is arguably of greater benefit.

3.1.3. The identification of critical information-sharing and decision-making channels and mechanisms within government and between the public and private sector.

Another important non-cyber facet relates to identifying the policies and procedures that are required to share information (Department of Homeland Security, 2006). Sharing information relating to a cyber incident, its vectors, payload, targets or source is vital to effective responses to cyber incidents. By staging an exercise organizers and participants can identify which information-sharing channels are effective, which pose bottlenecks to resolution and which need to be created.

This communication is of particular importance between the private and public sectors. A number of international exercises (*Cyber Storm* and *Cyber Europe* among them) specifically cited as goals for the improvement of communication between these two sectors. On the face of things this may appear to be obvious, but staging exercises that require effective communication, collaboration and information-sharing facilitates the identification of areas where channels are needed or should be improved, and can also highlight areas not previously known to participants.

The European Defence Agency recognized that such hidden communication channels are more prevalent between state actors. This is due to different legal frameworks and political priorities. What is germane and an important goal of staging such exercises is to identify options for collaboration (Röhrig, 2013). Differing regional, cantonal or national frameworks can work together if channels and scope for that co-operation can be identified. Staging simulated cyber exercises can achieve this.

3.2. Testing mechanisms and/or procedures

While identification refers to finding vulnerabilities, flaws, points of weakness or strength and uncovering channels of communication, *testing* refers to using these already identified elements in a situation to ensure that they are functioning correctly and do what they are intended to do. The use of simulated environments or scenarios in which to test software or hardware tools before deployment is a well-known technique both for the military and the computer technology industry. This can include defensive tools but also automated systems in a secure environment where failure of the system provides a learning opportunity, rather than having real-world consequences (Rapid7, 2017). The research also found that, in the context of cyber simulations, the "mechanisms" tested also refers to human actors, such as CERT teams or decision-makers, and their capacity to respond to particular cyber incidents.

Testing refers not just to evaluating technological resources to ensure that they are fit for purpose, however. As with the identification of procedural or legislative bottlenecks set out in Point 1 above, testing legal and regulatory frameworks to check they are fit for purpose is crucial, as is testing compliance to these frameworks. An example of this was the *Cyber Europe 2016* exercise, where, among other goals, the exercise sought to test EU Member States' preparation for

compliance with the EU's Directive on Network and Information Security[5] (Rapid7, 2017).

3.3. Exercising mechanisms and/or procedures

In contrast to the testing of new or established systems, resources and expertise, exercising those resources refers to their periodic deployment and use in a controlled, safe environment (Gomez, 2018) to prevent response atrophy or complacency, and ensure readiness in the event of a real incident taking place. The series of *Cyber Storm* exercises organized by the US DHS sought to exercise capabilities to ensure a state of readiness. While the testing of resources and mechanisms can demonstrate how well these subjects hold up to a particular type of incident, exercising them ensures that these resources maintain an effective state of readiness.

There are two elements which arose in the research which are worth examining separately. The first is that certain of the exercises staged specifically sought to exercise the readiness of high-level decision makers, several layers of bureaucracy above the front-line operators of cyber defense solutions. *Cyber Storm II* is a notable example of this. The goal was to test the capacity of the senior decision-makers in the various participating agencies to co-ordinate their responses within national and agency policy and procedural parameters. This is a notable exception to a number of exercises studied, which sought to test the *operational* readiness of CERTs and other cyber first-responders. Exercising leadership to prevent complacency but also to increase experience and awareness, particularly if there are changes in personnel in these higher echelons is an important component of institutional readiness and response capability.

The need to exercise senior-level decision-making capacities and the personnel with that responsibility was also recognized by the European Defence Agency. That Agency, however, went one step further. It also included cyber defense legal experts in its exercise goals. The intention of this inclusion was to fully integrate this expertise into cyber defense response process. This is particularly significant given a number of senior level decision-makers as well as front line operators may have the knowledge and/or willingness to use particular technical solutions and digital tools, but do not have the expertise necessary to identify the potential legal ramifications of one or other course of action. Exercising the triangle of co-ordination between technical possibilities, decision-making capacity and the legal footing to use certain resources can be an important goal of staging cyber defense exercises, one which arguably should always be recognized and included in planning, if not explicitly stated in exercise documentation and published aims.

3.4. Increasing communication and co-operation

Related to Goal 3.1.3 above, increasing communication, improving channels of information-sharing and facilitating co-operation between responsible actors are by far the most significant overall objectives and reasons for staging exercises. In a simulation or table-top exercise, it is not enough for participants to simply go through the motions and respond by rote, or to apply their own solutions in isolation from each other. Every participant discusses the situation with team-mates or colleagues and this horizontal interaction is encouraged. Throughout all the data gathered and researched for this Report, the importance of communication and co-operation is frequently repeated (CCDCOE, 2013, 2010; Department of Homeland Security, 2011, 2009, 2006; ENISA, 2017). The sharing of information is vital to a successful exercise and, by extension, to a successful response to a real-life cyber incident. Many of the points made in the AARs and interview data examined derive from a position of basic common sense, but having these notions spelled in this manner adds impact, clarifying the seriousness of this particular issue.

The AARs and interviews showed that coordinated, co-operative action and free-flowing communication are vital when responding to cyber incidents. The research found that there were particular references to the need for co-operation between different actor types. The European Defense Agency highlighted the need for civilian and military entities to work together more closely to the extent of aligning civil and military training curricula (Röhrig, 2013, p. 16), while the *Cyber Storm* exercises made repeated reference to the need for the public (i.e. government) and private, corporate entities to co-operate. Once again, this seems to be basic common sense, especially as the majority of the cyber infrastructure is owned and operated by private entities. Nevertheless, the core aims cited in the management and organization of the exercises was not just to promote the idea of co-operation, but to actively investigate current and new avenues for it.

What the exercises also did was to highlight bottlenecks to achieving this co-operation and co-ordination. One of those bottlenecks was a lack of effective communication. Communication between actors and the channels to facilitate this frequently appear in the statements of purpose and objectives of a number of international and national exercise AARs. In *Cyber Storm I*, communication was one of the three overarching areas along with response policies and

[5] More generally known as the NIS Directive

operational procedures being studies as part of the exercise (Department of Homeland Security, 2006, p. 3). In the case of NATO's *Locked Shields* exercises the need for effective communication between separate communities with vastly different expertise – in this case the technical community and legal experts – was also explicitly stated. The thinking behind this is that a multi-actor response to a large-scale cyber incident with the possibility of international consequences was only as good as the responders' ability to share information and communicate effectively.

The research showed that there are two important benefits for conducting simulated cyber exercises for communication. One is the need to identify barriers to effective communication between responding actors. Simulated cyber exercises of any scale and nature – whether multinational simulations or small-scale table-top exercises conducted within a private company – all help to identify where communication bottlenecks occur, in particular those which hinder clear and effective information-sharing channels. While a number of government actors have in place the capacity to share information between departments (Baezner, In Press; Cordey, 2018; Dewar, 2018), the involvement of the private sector highlighted issues relating the sharing of classified, proprietary or customer data (*Cyber Storm II*, p. 8). Responding to simulated cyber incidents was occasionally hampered by a lack of clear political leadership in these exercises, something that could have severe implication for the effectiveness of real-world responses. The exercises studied did not in the main provide solutions to this bottleneck as the procedures for establishing this level of information-sharing and the operation of those procedures are political decisions. The goals of the exercises staged were to identify in which specific areas these political decisions needed be made.

The second component often cited in the AARs and interviews is the need for effective decision-making infrastructures and the capacity to communicate those decisions (Department of Homeland Security, 2011, p. 20; ENISA, 2011, p. 24; Haggman, 2018b). In one example it was found that the procedures in place for decision-making – feeding information and recommendations up bureaucratic ladders, analysis of options and the feeding of response decisions back to the operators – was cumbersome and not conducive to responding to real-time, fast moving simulated incidents. Once again, this had implications for the capacity of the actors to respond to real events. In both of these examples the goals of the exercises were to identify potential bottlenecks in a simulated environment so that they could be remedied and not cause difficulties in a real-life cyber incident.

3.5. Developing policy

The final trending goal of staging exercises is often overlooked in statements of intent, but analysis of AARs and interviews with organizers and participants highlights its importance. A corollary to identifying gaps in current policy frameworks, or bottlenecks in policy that hinder effective responses to cyber incidents, is the use of exercises to develop policy where none currently exists. While it may appear to be very similar to these other two activities, the specific goals are very different.

When identifying policy or procedural issues (see 1.2 above) a framework is already in place. The goal is to examine that framework and work out what works and what does not. When establishing *policy development* as a goal the aim is to use the experience of participating in a simulated event to build the framework itself, often from scratch. The purpose in such situations is not to test technical responses nor technical expertise, but to focus on the policy frameworks in which these technical responses could be used. This was a central aim of the *Cyber 9/12 Challenges* of 2018, one hosted in February by the Atlantic Council and another hosted in March in Geneva by the Geneva Centre for Security Policy (GCSP). These exercises were competition-based, with contestants tasked with developing policy frameworks from the ground up in a fast-moving, simulated cyber incident. The goal of the exercise was to train participants in policy-making in real time in a simulated, controlled environment. Technical, digital solutions and infrastructures were not the focus of these exercises, as opposed to the other exercises examined for this research. Equally, the developed was itself simulated. The solutions proposed remained in the artificial, simulated environment of the competition, and the winning solutions were not translated into the real world. Despite this controlled environment the exercise was successful not only in making participants aware of the nuances of policy frameworks, but also that cyber security and defense are not solely technical issues. While policy was an important aspect of *Locked Shields, Cyber Storm, Cyber Europe* and *Baltic Shield*, the primary focus was placed on technical solutions and the capacity of team to respond to a cyber incident from a technical perspective. The focus of *Cyber 9/12* was purely policy.

An advantage of policy development exercises such as *Cyber 9/12* is that it does not require large amounts of technical resources to mount, nor does it require a high level of technical skill on the part of the participants. That being said, interviews with organizers of the *Cyber 9/12 Challenge* found that technical experts are encouraged to participate precisely because there is little technical activity being undertaken. Expanding the experience base of those with direct operational tasks in responding to cyber incidents is universally agreed to be beneficial.

3.6. Exercise audiences

An important consideration for the staging of exercises is its audience. This does not mean which participants will contribute the most or get the most out the exercise, but who is it that ultimately benefits from such exercises – at large or small scale – being carried out. The most obvious beneficiary of such exercises are governments, public sector departments and private organizations tasked with crisis and disaster management, national security or defense. Such organizations are frequent participants in exercises and use them to drill their staff or increase co-operation with partner bodies (ENISA, 2015, p. 22). Both large and small exercises are an important part of these organizations' preparedness (Australian Institute for Disaster Resilience, 2012).

There are wider beneficiaries as well. By actively engaging with the (real-world) media and encouraging media reporting governments can demonstrate that actions are being taken to enhance cyber security and improve preparedness should a cyber incident take place (ENISA, 2012b, p. 13). This will go some way to boosting public awareness of national activities and preparedness and thereby boosting public confidence in the capacity of organizations to respond should an incident occur.

4 Types of Exercises

This chapter examines the types of cyber security exercises which can be selected by first dividing these exercises into two main groups: full simulations and table-top exercises. Full simulations are resource intensive and generally utilize some sort of technical representation of an incident, while table-top exercises are predominantly discussion-based with a reduced focus on technical or technological matters. Within these two over-arching groups there are a number of specific exercise activities, each with their own advantages and disadvantages, resource implications and objectives. The chapter examines three of these types which frequently occur in the literature. These are Capture the Flag scenarios, "red-teaming" and workshops.

This chapter is not intended to provide an exhaustive list of the kinds of exercises or activities which organizers can undertake. The objective of the chapter is to provide an understanding of exercise types and the goals that these activities can achieve, important considerations to be borne in mind by those entities staging or planning to stage cyber security exercises. The exercises examined as summarized in Table 2 below.

4.1 Full Simulation or Table-top Exercise?

One of the key findings of this Report is that cyber security exercises can be divided broadly into two types:

1. Full-scale simulation reflecting as close as possible a "real life" situation
2. Table-top or paper-based exercise

Both types of exercise have intrinsic advantages and disadvantages. Full-scale simulations can involve the use of virtual network environments enabling participants to experience a cyber-incident in a controlled manner. Such exercises are, however, resource-intensive and require extensive planning. Table-top exercises can take up only a few hours, but are generally discussion-based and so the sense of urgency and realism provided in simulations is lost.

4.1.1. Full Simulations

Full simulations replicate real world situations. The utilize representations of attackers or incidents, virtual, artificial computer architectures and network intrusions in order to provide a "reasonable representation of a real environment" (Krain and Shadle, 2006, p. 52). The idea is that during the exercises participants will be faced with situations which reflect the kinds of incidents they would face in the real world, in the kind of network architecture in which they would be required to work. Within the scope of a particular, pre-defined scenario, technical resources are made available so that participants can experience simulated incidents in real time. These include the effects of, for example, a cyber-incident targeting on an element of critical infrastructure. This enables participants to be able to respond to a real-life incident should one occur.

Simulations are often adopted by those organizing cyber war-games, involving the drilling or training of military and security personnel. These types of games are a cyber version of the kind s of activities well-known in the military (see Chapter 2.1 above). One type of cyber exercise that can utilize a full-scale

Table 2: Types of Exercise and Exercise Activities

Type of Exercise	Description
Full Simulation	Simulation of a real environment with a virtual or secured digital network in which to conduct exercises using real tools and techniques
Table-top	(Usually) non-technical, discussion based exercise which can employ evolving scenarios but with a lesser focus on technical solutions to simulated events

Types of Exercise Activity	Description	Full Simulation or Table-top?
Capture the Flag (CtF)	A form of war-gaming where participants are divided into red and blue teams, with red teams playing the part of the aggressor or hacker and blue teams defending.	Full simulation
Red-Teaming	An activity is an audit of an organization for compliance purposes or to measure that organization's level of preparedness.	Full simulation
Workshop/seminar	Discussion-based table-top exercise not normally associated with full technical simulations.	Full simulation/Table-top

simulation is an activity known as "Capture the Flag" (see section 4.2.1.). In this exercise participants are divided into red teams (attackers) and blue teams (defenders) and operate within the same network environment. In addition, depending on the scale of the simulation and the exercise, the organizers may have their own white, green or yellow teams to provide infrastructure support or communications with the media and the participants.

Because full simulations tend to require a virtual or at least secured network environment in which to conduct the scenario, they require substantial digital hardware to stage, and that hardware must be maintained. As such they are resource-intensive: a virtual digital environment to be created and maintained, and non-scenario failures or incidents must be minimized. This means that a dedicated, non-game IT support staff is required to ensure that no failures of digital infrastructure occur that are not part of the game play. Any servers, computers, laptops, electricity requirements and host venues required must therefore be of a scale suitable to the goals of the exercise and the numbers of participants. A comprehensive cost-benefit analysis must therefore be carried out if a full simulation is being considered. Although they are attractive cyber exercises as a result of the potential for training participants in as close an approximation to real-life as possible, the costs of staging a simulation may far outweigh the benefits given the exercise goals. Policy development, for instance, is perhaps not best served by a full-sale, technology-heavy simulation.

4.1.2. Table-top exercises

In contrast to full, technological simulations, table-top based exercises usually involve a hypothetical scenario (as will full simulations) but without a technological element. Table-top exercises are discussion-based and usually involve round-table discussions of potential cyber events and possible solutions. Examples of established table-top exercises include the *Cyber 9/12 Challenge* hosted by the Geneva Centre for Security Policy and the Atlantic Council (GCSP, 2018) and "The Great (Cyber) Game", developed by Andreas Haggman as a way of training cyber security personnel without the need for a virtual environment.

The objectives of table-top and other BOGSAT exercises are not necessarily to drill personnel or test technical solutions or preparedness, but to enable discussions around policy solutions without the pressure of constant attacks from a red team. Without this pressure and time constraint, the focus of the exercise can shift to more abstract solution-building or policy development.

An additional advantage of table-top exercises over simulations is that, because there are fewer resources needed these table-top exercises can be of almost any scale, ranging from internal, one-hour discussions within a corporate IT department to three-day events with multiple international participants, such as the *Cyber 9/12 Challenge*. This format therefore has greater flexibility than simulations. As a result, table-top exercises are available to a larger participant demographic. Because they can be of a smaller scale and last only a few hours, chief-level (C-Suite) executives from a private corporation or general-rank staff in the military can take part and the exercise can still have positive outcomes. This demographic are often not amenable or available for highly involved, technical, full-scale simulations spanning days (Haggman, 2018b)[6].

4.2 Specific types of exercise

Within the scope of these two broad categories there are specific activities which can be undertaken. There are numerous different types of activity, and different variations on themes. Three main types are presented and described here. The objective is not to produce an exhaustive list of activities, but to present an indication of the kinds of exercises which can be conducted. It is important to note that all of the types mentioned here can be conducted either as full simulations or as table-top activities, depending on the needs of the organizers and the goals of the exercise.

4.2.1. Capture the Flag

"Capture the Flag" (CtF) activities are often selected for large, international exercises, such as *Locked Shields* or *Cyber Europe*. CtF is a form of war-gaming where participants are divided into red and blue teams, with red teams playing the part of the aggressor or hacker and blue teams defending. Depending on the nature of the scenario, blue teams may be required to work together or independently to achieve game goals. In game play, teams are awarded points depending on how deep they penetrate a defended network or how swiftly they respond to and remedy an incident or attack.

Although most often conducted in a full simulation such as *Locked Shields* or *Cyber Storm*, in his "Great (Cyber) Game" Haggman (2018b) demonstrated that the CtF format can also be used in a table-top activity for teaching and awareness purposes. This vastly reduces the resources required to stage an exercise. Removing the technological component however, also vastly changes the exercise parameters, and affects the goals which can be achieved. Once again, the nature of the exercise depends on the goals

[6] Although this does occur, depending on the level of personal interest and investment from the senior staff.

4.2.2. Red-teaming

According to Gomez (2018), red-teaming as an activity is an audit of an organization for compliance purposes or to measure that organization's level of preparedness. As such it can be either a full simulation or desk-based. Once again, the nature of the exercise is contingent on the precise goals and objective of the audit.

It must be pointed out that Red-teaming is not the same as a red team/blue team competition scenario. Although the names are similar and this similarity can cause confusion, red-teaming is a specific type of activity with specific, defined goal: to seek to penetrate an entity's defenses deliberately and with that entity's knowledge in order to test procedures or identify weaknesses. As discussed in Section 4.2.1, red team/blue team exercises such as CtF are war-game style competitions, pitting teams against each other, rather than a single defended entity.

4.2.3. Workshops and Discussions

These exercises are primarily desk-based paper activities. They are useful for policy analysis and identifying communications bottlenecks as they can be conducted without or with a minimum of technological input. As such, they are beneficial for C-suite and military general staff as such exercises need not be time-consuming and require a minimum of preparation. They can be conducted in a matter of hours rather than days for some simulations. That being said, depending on the goals of the exercise, a certain degree of technical input can be pro

These can be workshops or seminars, with more or less participation and interaction from the participants. ENISA classifies workshops as a third, separate category to discussions and table-top exercises by arguing that workshops are a rehearsal for table-top activities and more advanced scenarios (ENISA, 2015, p. 19). Workshops are classified together in this Report as they are, by their nature, table-top activities. They may utilize a scenario to work through but tend not to employ the kinds of technical resources found in full simulations.

4.3 Considerations when selecting an exercise type

The most important factor to consider when selecting an exercise type is that the type selected depends on its overall goals: what do organizers wish to do and achieve? If the goal or objective is to test technical solutions for particular forms of cyber-attack or cyber incident, a full simulation is arguably the most appropriate type of exercise given its ability to reflect real-life events. If, however, the goal is to develop or test policy solutions, then a table-top, BOGSAT exercise may be just as effective, or even more so given the removal of the focus on technological elements of the system.

Another important consideration is the style of learning involved in the exercise. As discussed in Chapter 2.2, active learning techniques such as interactive simulations and scenarios requiring more direct involvement of participants promotes better understanding and use of techniques, theories and concepts. As a result, full simulations – which are highly conducive to active learning – are an attractive format for a cyber exercise. Such a focus on learning may not, however, be the primary objective or goal of the exercise organizers.

It is clear therefore, that certain goals lend themselves to one or other type of exercise. As shown in this chapter, however, both table-top and simulation activities can be applied to certain goals. Red-Teaming does not necessarily require a full simulation to be carried out, particularly if the organizer is a smaller entity, such as a small or medium sized enterprise (SME) or individual government ministry. The entity staging the exercise may simply not have the resources required to stage a full simulation. However, if the Red-Teaming exercise is intended to audit national resilience, disaster management or incident preparedness, then a full simulation may be prudent to test the maximum number of resources

It is therefore important to ensure that the scale of the exercise matches the objectives. If this is the first time a response team is convening, a workshop or scenario-based table-top activity could be more suitable than jumping straight for a full-scale simulation. ENISA notes such activities as being lower down the resource spectrum (ENISA, 2012b, p. 9) and are therefore cheaper to run.

The target demographic for the exercise must also be kept in mind when selecting an exercise type. C-Suite executive in a corporate environment or high-ranking military personnel may not have more than a few hours to spare, therefore a full simulation may not be the best use of resources, despite the fact that simulations can have the greatest impact in terms of presenting findings regarding cyber vulnerabilities. The consequence of all these considerations when selecting an exercise type is that an effective cost-benefit analysis must be undertaken setting the goals to be achieved alongside the resources needed to stage a particular exercise type. Full simulations are costly to plan, implement and conduct, while table-top activities are significantly cheaper. The goals of the exercise must be balanced with the actual needs of the organization staging the exercise.

5 Resources

Resource requirements for staging a successful exercise are also highly contextualized; the amount and nature of resources required is dependent on the nature of the exercise, its goals and the demographic of its participants. The AARs and interviews examined for this Report did not offer general or generic resource needs. What is necessary and crucial to the success of one type of event may be irrelevant for another. Nevertheless, there are certain "basic" resource considerations which organizers should be aware of when staging exercises. These are:

- The "basics" of an exercise comprise hardware, software and incidentals such as catering and stationery, but as each exercise is unique, the precise combinations of these will differ.
- Each exercise requires an efficient, well-organized and effective supporting infrastructure, with clearly defined areas of responsibility.
- Regardless of which resources are selected or deemed necessary, *adequate amounts* of a resource is vital. Repeatedly AARs and interviews stated that there was not enough of one resource or another, and such lacks caused functional problems for the exercise.

5.1 The "Basics" of organizing events

Although each cyber security simulation or exercise is unique. Each exercise will have different goals and different participants meaning that each exercise has different resource needs. That being said, there are basic resources which all exercises should at least provide or have access to. These are hardware (desktop computers, laptops, servers or other communications devices), suitable software (especially if running a full simulation) and incidentals (stationery, a venue, catering). The nature of the exercise, as dictated by its goals, will also affect the precise amounts combinations of these resources.

There are also general rules of thumb when organizing such events. Some of these are obvious: the larger and more complex the exercise, the greater the resource needs (Cederberg, 2018). Table-top exercises can be conducted over a few hours in a single room, while full simulations require an artificial network to be constructed and maintained by a dedicated platform. This was the option utilized when the Czech government carried out their cyber security exercise in 2015 (Vykopal and Mokoš, 2016, p. 22). In its research on cyber exercises ENISA produced an initial classification of exercises based on an increasing scale of resource intensity (ENISA, 2012b, p. 9). While that classification did not cover all the nuances of exercise types in order to create an effective taxonomy, it does provide a baseline for resource allocation and requisition. At the lower end of resource intensity are small-scale, internal discussions with minimal resource requirements beyond a location and stationery, while at the higher end are full simulations with multiple participants. The selection of an exercise type and subsequent resource requisition relies heavily on the goals the exercise is to achieve.

It must always be borne in mind that each exercise is therefore an individual event, with. Beyond these basics exercises' resource needs should be agreed on a case-by-case basis, with a clear understanding of the goals and objectives of the exercise informing which resources are required to best achieve those goals.

5.2 An effective, well-resourced supporting infrastructure is needed

A common theme identified in the data sources is that having an effective organizer infrastructure in place is crucial to the smooth execution of the exercise, both at the planning stage and as the exercise is being conducted. The most important aspect of that infrastructure is ensuring that management and maintenance responsibilities are clear. While each exercise is unique and has its own goals and resource idiosyncrasies, having a clear management structure and hierarchy, with clear delegation of responsibilities for particular tasks, can ensure a smooth and successful exercise. This includes responsibilities the necessity of which is not immediately obvious. For example, beyond IT specialists able to maintain the virtual exercise environment, the organizers of the *Locked Shields 13* exercise included provisions for legal advisors to brief Blue Team defenders on their legal status, rights and obligations (CCDCOE, 2013, p. 41). This ensured that any actions taken by the Blue Teams were realistic, in the sense that they were legally able to be used.

There are four resource implications here: first, for *Locked Shields 13* there was a need for specific expertise that necessitated a dedicated team, in this case legal experts; second, such bespoke teams will require additional resources beyond those of the technical maintenance teams; third, the requirement for these bespoke teams needs be identified at the planning stages of an exercise, but will require extra foresight in those planning stages and can only be drafted in during game play at considerable expense; finally, there needs to be enough staff to fulfill the responsibilities allocated to these bespoke teams. The *Locked Shields 2013* AAR (2013, p. 54) noted that there were not enough legal advisers, despite their presence having been pre-planned.

The *Locked Shields 2013* AAR provides a detailed breakdown of the responsibilities necessary for a successful Red Team-Blue Team exercise involving a simulated cyber event and serves as an example for

prospective organizers. Given the scale of the *Locked Shields* itself, these responsibilities were assigned to dedicated teams, however the actions can be carried out by a single team if the exercise is of a small enough scale. What is germane here is that these are the key responsibilities necessary for an effective, successful exercise, whether they are concentrated or distributed. This is summarized in table 3.

The key takeaway here is that what is most important is for the responsibilities or functions of the support teams to be clarified and handled. Depending on the scale of the event and the nature of the tasks, these responsibilities can be covered elsewhere. For example, in an internal private event a separate legal team may not be required as the white team will be able to take on this responsibility. Alternatively, a corporate entity may have its own in-house legal department, with those staff able to take on the responsibility of providing response advice in an internal exercise. In addition, and internal IT department can act as its own Green Team.

Certain resources necessary for a functioning infrastructure are more abstract. A crucial aspect of the infrastructure is an effective, believable and flexible scenario (Egloff, 2018; IAEA, n.d.). Whether it is used for a full-scale simulation or a small, two-hour table-top exercise, the scenario in which the exercise takes place must be believable: it should contain incidents that could conceivably happen in real life. This requirement often precludes the most devastating of cyber-incidents as such incidents have not occurred in real life and are considered unlikely to occur (Rid, 2013) given the current state of national and corporate cyber security measures. Therefore, the exercises that are the most successful and effective are those that realistically portray real-world events.

This requirement has a potential knock-on effect: it has an impact on the roles participants play in the exercises. If the participants are not representing themselves (as is the case with the majority of *Cyber Storm* exercises) then a backstory for each group pertinent to the scenario is beneficial (Vykopal and Mokoš, 2016). This must also be believable, and a conceivable occurrence in reality. There is no benefit to attributing vast arsenals of highly complex and damaging cyber weapons to a particular actor if the role they play is not commensurate to their capabilities.

Finally, the infrastructure supporting the exercise must reflect the needs of the scenario but also allow enough flexibility to enable the scenario to develop naturally and organically (Haggman, 2018b). Haggman and the International Atomic Energy Agency (IAEA) both recommend that any scenario be flexible enough to allow for free-play, meaning participants should be able to be as creative as possible when developing solutions, rather than restricted to a few specific measures (IAEA, n.d.). The onus here is on the organizers and exercise monitors to balance ensuring the needs and goals of the exercise are met with enabling participants to be as creative as possible in their solution development.

Table 3: Basic Resources and Responsibilities Necessary for a Cyber Exercise

Basic Resources	
Staff	This includes planning teams, event management staff and others charged with specific responsibilities (see below)
Hardware	Computers for participants AND organizers; servers for simulations; Wi-Fi
Communications infrastructure	Particularly relevant for distributed exercises
Software	Specifically for simulations
Venue	Suitable for size of exercise
Incidentals	Catering; stationery for participants
Responsibilities	
Team	Responsibilities
White Team	Prepares and executes the exercise; includes media relations (called Logistics Team by Australian Institute (Australian Institute for Disaster Resilience, 2012)
Blue Teams	Participants, usually defenders
Red Team	Antagonists (the bad guys). Considered a work-force team because the objective of *Locked Shields* is to train Blue Teams
Green Team	Prepare and maintain technical infrastructure
Yellow Team	provides situational awareness to other teams

5.3 Adequate resources are crucial

A common refrain in the AARs and interviews examined for this Report is that *enough* resources are necessary for a successful exercise. This point may seem obvious and self-explanatory but the number of times AARs state that there wasn't enough of resource X or the numbers of staff with expertise Y was insufficient make this a point worth highlighting. At one level organizers need to ensure that the infrastructure they have set up to operate and maintain the exercise can cope with the demands placed upon it. The hardware for the network infrastructure must be able to cope with demands of the exercise as it unfolds, especially in the case of a full simulation. Some exercise organizers found that their virtual network could not cope with the demands of the exercise (as was the case in *Locked Shields 12*) towards its latter stages. Not only could this have compromised the infrastructure and the goals set for the exercise, but such a situation would lead to a sub-optimal exercise experience for the participants, making a repeat of the exercise unlikely. The national exercises conducted by the Czech Republic were quite candid in this regard, and noted that that there were not enough network hosts for the White Team organizers themselves (Vykopal and Mokoš, 2016). In addition, some exercises reported that there were not enough technicians on hand to maintain the virtual network causing non-scenario technical issues. While it was noted that staffing levels were adequate during the preparation process for *Locked Shields 13*, during the exercise itself the Green Team of in-house technicians could not cope with the workload of information and technical requests (CCDCOE, 2013). Having enough staff on-hand can also mean having enough White Team members to explain scoring decisions or field calls from the media, in order that participants can concentrate on the exercise itself. Large-scale multinational exercises can attract a great deal of media attention that must be effectively managed. Similarly, some Blue Team participants in *Locked Shields 13* pointed out that they were unclear as to why specific scoring decisions were made (CCDCOE, 2013, p. 56). Part of the problem was that Yellow Teams with this decision-making responsibility did not have enough staff to ensure these details were efficiently communicated.

Management of responsibilities and staffing is therefore also crucial. Technical support and media relations are responsibilities that need to be addressed during the exercise. Depending on the scale of the exercise these can be carried out internally by one team (small exercise; corporate or internal to a ministry) or have separate teams set up to focus on one particular responsibility (large exercise e.g. *Cyber Storm/Cyber Europe*). However, effective resource management must also be undertaken and can provide creative solutions to resourcing issues. Large multi-actor simulations can require more intensive infrastructure resources. A distributed exercise, however, may require fewer resources due to participants being able to use their own equipment in their own location (Hoffman et al., 2005). In distributed exercises, incidentals such as venues, catering and accommodation are also minimized. One downside to such a style of exercise is that communications then becomes crucial. The US *Cyber Storm* exercise of 2016 involved 1200 participants over numerous locations, requiring substantial and complex teleconferencing systems to be provided and maintained (Department of Homeland Security, 2016).

Exercise organizers and planners need to bear in mind the levels of resources they have and ensure that there is enough to achieve their objectives. It is recommended that first-time planners, or exercises being run for the first time should start with small, easily achievable goals and steadily work up to large-scale simulations (if that is the ultimate aim). These resources can be as simple as having large enough desks for suitable equipment (CCDCOE, 2012, p. 55) or rooms large enough to host full teams for debriefs. In the lessons learned section of the AAR for *Locked Shields* 2013 (2013, pp. 58–59), it was recommended that servers made available for future exercises be of increased capacity to minimize the risk of non-scenario technical failures.

6 Actors/Participants

A crucial element of organizing exercises is selecting the correct demographic of participants. Drawing participants from a variety of (relevant) backgrounds leads to exercises which are more rewarding for the participants but which also yield more beneficial findings for organizers (Haggman, 2018b). Information gathered from event AARs and expert interviews found that there is large number of individual actors and entities who take part in simulated events. The examination of AARs from American events such as *Cyber Storm* or European events such as *Cyber Europe* cites over 100 individual corporate, public sector, government, military or security entities in their participant lists.

This chapter examines four important points to consider when organizing and staging events: first, that there is no ideal demographic for participation – that demographic depends to a large extent on the agreed goals of the event itself; second, despite there being no ideal demographic, there are several entities which routinely participate in exercises; third, while the goals of the event to an extent dictate the demographics of participation, that demographic can also impact on whether the event itself is a tabletop scenario or a large-scale simulation; fourth and finally, a relationship with the media is crucial. Some exercises may include classified elements due to their goals or participants, but keeping the media at arms' length is not advisable.

The chapter closes by providing some advice on meeting the challenge of participant selection in order to stage as successful an exercise as possible.

6.1 Who participates is highly dependent on the goals of the event

The research found that actor participation is highly context-dependent with an actor's participation contingent on factors relating to the event. Military or national security actors tended to focus on war-gaming scenarios in order to ensure combat or incident readiness, or to provide training in new tools and techniques. Private corporations tend to focus on penetration testing, as their ultimate goal is to prevent unauthorized access and exfiltration of data. The demographic of participants is therefore contingent on the goals of the event itself, and what was to be tested or exercised dictated which actors were invited and encouraged to participate.

This also had a bearing on the numbers of actors involved. Where increasing communication or identifying bottlenecks to that communication was one of the core goals of the event, then a wide range of actors with interests in the type of scenario were invited to take part. If the scenario was an attack by an enemy state on an aspect of critical infrastructure, then national security and military actors tended to be more heavily involved, as were representatives from the private sector which owned the infrastructure. In all cases, actors were not invited to participate simply for participation's sake, but in order to ensure that a relevant contribution was made to the overall goals of the event and therefore to cyber security itself. The challenge for organizers is how to decide which participants to invite.

6.2 The "usual suspects" of simulated cyber events

Despite this highly contextualized participation, a standard content analysis carried out on literature and interview sources found that there are a number of actor types which frequently participated in the events examined. These are entities which regularly or routinely take part irrespective of the goals to be achieved or the systems to be tested. These "usual suspects" are:

- National government actors including defense ministry, interior ministry and energy ministry representatives
- Military personnel
- National security agencies
- Private sector entities, in particular telecommunications and energy firms,
    - Also includes Information security entities (such as FireEye, Symantec etc. and also hardware producers)
- National CERTs
- Academic representatives

This list of regular participants in cyber exercises demonstrates the importance placed by national governments on cyber security and cyber defense events, but also the positioning of these to policy areas within wider frameworks. The wide range of individual actors participating in simulated and scenario-based events points to a recognition of the need for holistic solutions to cyber defense problems. This indication is countered, however, by the repeated participation of defense and security-focused government entities in international simulations.

What this list does not demonstrate, however, is the complicated nature of private sector involvement in cyber exercises. On the one hand, much of the infrastructure underpinning the Internet and the World Wide Web is owned, operated and maintained by private sector corporations in the telecommunications industry. This makes these organizations a logical invitee to cyber security exercises. However, the involvement of military and national security entities in some exercises makes such involvement complicated. Access to classified capabilities and tools must be closely

monitored. As a result, private sector entities are not always invited to participate. The AAR for *Cyber Europe 2010* pointed out that private sector were initially omitted, this time due to time constraints relating to planning and delivery given that this was the first pan-European exercise (ENISA, 2011, p. 43). While this was considered a valid approach at the planning stages, ENISA acknowledged that there was an almost unanimous agreement that this omission was a mistake and caused a disadvantage to the overall exercise by not making it as realistic as it could have been. To make future exercises as realistic as possible, participants unanimously agreed that the private sector should be a part of those future exercises. Organizers pointed out that this would require extra co-ordination but that that coordination would pay dividends.

By the time ENISA published its Report on National and International Cyber Security Exercises in 2015, the emerging trend in such exercises was for closer and more integrated co-operation between the public and private sectors to the extent that a number of exercises (Cyber Guard and Cyber Attack and Business Continuity) specifically sought to encourage this form of co-operation (ENISA, 2015, pp. 23–24).

6.3 Goal-Actor interdependencies when organizing events

The goals and objectives of the events dictate the demographic of the participants. If an actor's participation is not germane to an event's larger objectives, then there is no specific benefit to their involvement except for networking between actors. While this is important, it must be taken into account in a cost-benefit analysis prior to the event being staged.

However, participant demographics can have an impact on the nature of the event itself, i.e. whether it is a tabletop exercise conducted over one or two-hours, or a simulated cyber-incident taking place over two or three days with high levels of technical expertise required on both sides. Both Haggman and Cederberg stated (independently) in the private sector C-suite executive education programs are recognized as beneficial in setting out core themes and security concerns, particularly in a field such as cyber security which is still considered a technical area (Cederberg, 2018; Haggman, 2018b). Haggman pointed out, however, that C-suite executives are often unable (or unwilling) to devote more than a few hours to the key aspects of a problem area. These time and availability constraints are brought into even sharper relief when staging events targeting high-level government ministers or even Prime Ministers. This nuance of participant demographic can also effect exercise resources regardless of goals of exercise. Highly-technical, resource-intensive simulated events reflecting real-world scenarios and taking place over a series of days are simply not feasible or practical for such actors to participate in, despite the potential returns. A process of re-evaluation and re-examination is therefore needed to ensure the balance is stuck between achieving (and achievable) event goals, actors' willingness and ability to participate and the resources needed to stage an effective exercise. Reducing the scope of the event may make involvement more appealing to these high-level actors, but will have an effect on the scale of the goals and objectives able to be achieved.

6.4 Relationship with the media

The final actor of importance in the staging of cyber events is the media, for several reasons. Media outlets are recognized as important components of cyber security and cyber defense. Several of the AARs examined cited social media and fake news campaigns as a component of the simulated event, with participants needed to control the media narrative to avoid either a spread of the incident vector or the spread of disinformation. Media outreach campaigns also offer opportunities for government entities, industry partners and other stakeholders to use findings to develop a public information strategy (Australian Institute for Disaster Resilience, 2012, p. 14). Liaison with the "real media" in this fashion can provide effective methods to educate the general public and raise awareness both of the events themselves but also of important aspects of cyber security and cyber defense that the general public needs to know.

Typically, however, the media are not involved as active participants (or even as primary observers), but are provided with information by White Teams detailing the progress of the event. On the one hand this is not surprising given that tools and techniques available to actors are often kept under very controlled circumstances. This is particularly true of military cyber capabilities. On the other hand the majority of the events examined had some sort of media component in the scenario – either a media entity was the victim of a cyber-incident or their platform was used as a vector for an incident. This is perhaps an indication that exercise organizers are still reconciling the integral role of media outlets and companies to holistic cyber security with the potential that classified capabilities may become known in the event that a media entity participates in a simulated event.

This lack of reconciliation is highlighted by the fact that, despite the usefulness of outreach campaigns, media organizations are frequently cited as an element that needs to be carefully managed. This management comes in two forms. White Team personnel and technical resources must be allocated to provide a direct link to media outlets reporting on the events, assuming the events are conducted in the public domain. In a similar vein, post-event media debriefings are important to maintain a sense of communication and connection

with the general public, the ultimate referent object of cybersecurity and cyberdefense policy. On the other hand there is the need on the part of the organizers and participants to remain in control of the media narrative and prevent any distortion of the objectives of the event. The general consensus appears to be, therefore, that event organizers and White Teams need to be both wary and effective when engaging with media outlets. This is a fine line to walk, and one which also requires resources and careful preparation.

6.5 The challenge is which participants to invite

Participant demographics must reflect the nature and objectives of the activity. This means that a reasoned decision-making process on participants should balance diversity with relevance. The greater the variety of backgrounds brought to the event, the greater the chances of creative solution- or network-building (Haggman, 2018b). However, as stated above, the demographic depends on the goals of the event, whether they are testing tools or capabilities, exercising already established teams and procedures or identifying and opening channels of communication. If the goal of the event is to test the capacities of a network internal to a private company or single government ministry, then inviting a range of participants may not be optimal, particularly given the possibility of external actors accessing classified or proprietary data. A balance must therefore be struck between the needs of the organizers, the parameters of the event and the likelihood of participation of key actors. The right or appropriate level of balance is a decision which must be made as early as possible in the planning stage.

The key issue to striking this balance when organizing or staging events is to know your audience; a certain degree of a priori knowledge is required to stage an effective event. This means having an understanding of the kinds of participants who would bring the most to a given event, as well as those who would benefit the most from the event's parameters at the commencement of planning and an awareness of those actors' capacities to engage with the event. This two-way involvement – ensuring that participants bring something to the event as well as learn something from it – is crucial to ensuring an effective, useful and enjoyable experience for participants.

Table 4: Actors regularly participating in Cyber Exercises

Actor	Description
National government entities	Government ministries
Military personnel	Personnel from all branches of a national military service
National Security entities	Non-military security actors, includes bodies such as the US Dept. of Homeland Security
Private Sector	Private corporations including telecoms providers, cyber security specialist firms, critical infrastructure providers (energy, transport etc.)
National CERTs	Computer emergency response teams at national and government-agency level
Academia	

7 Conclusions and Lessons Learned

This Report examined core features of cyber security and cyber defense exercises with a view to identifying important trends in resourcing such exercises, their goals, the nature of the participants involved and the types of exercises available. The collected findings of each individual chapter of this Report are summarized in Table 5 below where the goals, activities, resources and participants involved in cyber exercises are set alongside one another. The table demonstrates the challenges in identifying a one-size fits all combination of resources, actors, goals and participants for cyber exercises because it is not possible to produce a "shopping list" for exercises, where a planner can take a goal from one column, an activity from another, combine them with a specific actor demographic and produce an effective exercise. Each exercise is individual and must be treated as such. It must be tailored to the goals the organizers wish to achieve, goals that must be established and clearly articulated early in the exercise planning phase.

The research did yield a number of important findings however. First, an understanding of context is crucial: each exercise is unique, with resources required and participant demographics heavily contingent on the idiosyncratic goals of the exercise itself. Second, effective planning stage is crucial to the success of an exercise. This includes early and clear exercise goal definition. Third, where scenarios are to be used in an exercise, they must be realistic and not always resort to the worst possible combination of events. Fourth, cyber ranges are notable by their absence in the AARs and interviews examined for this Report, to the extent that, in the context of cyber exercises, such ranges are not the top priority. Finally, there were warnings against conducting exercises simply for the sake of conducting exercises. Each exercise must serve some purpose and that utility must be clearly defined.

7.1 Context is crucial

The most important finding of the research for this Report: there is no "one-size-fits-all" combination of resources, goals, participants and exercise types that can be routinely applied to cyber exercises. Equally, there is no one exercise type that can be used for all education and training purposes. Each individual exercise is unique, and tailored to the specific goals of that exercise – to its context. All decisions relating to the conduct, staging and resourcing of the exercise stem from having clearly established goals. As a result, the goals of an exercise must not only be clearly stated but established an agreed upon as early in the planning process as possible. These goals can be simple (such as testing a specific tool) or highly complex (such as facilitating co-operation between multiple international entities). Whatever the case, exercise goals must form the foundation for the development of an exercise because what the organizers seek to achieve in an exercise dictates all other aspects of the exercise

Table 5: Summary of findings

Goals	Types of Exercise*	Resources	Responsibilities	Participants
Identification	Full Simulation	Staff	Preparation and execution of exercise	National government entities
Testing mechanisms and procedures	Table-top	Hardware	Defenders and attackers (in a red team/blue team activity)	Military
Drills	CtF	Software	Maintaining technical infrastructure	National Security entities
Increasing co-operation and communication	Red-Teaming	Communications infrastructure	Inter-team communications and situational awareness	Private sector
Developing policies and procedures	Workshop/Seminar	Venue		National CERTs
	Red team/Blue team	Incidentals (catering, stationery)		Academia

*Full Simulation and Table-top (blue) exercises are the two overarching types of cyber security exercise which can be conducted. The remaining items in this table (green) are the various activities which can be conducted as *either* simulations *or* table-top exercises.

including the activities the participants would undertake and thereby the nature of the exercise itself.

7.2 Planning is key

As indicated in Section 7.1 above, planning is crucial to the success of an exercise. All the goals of the exercise must be established early as these determine a context for the exercise as a whole: which resources will be required; how much of those resources; which participants to invite etc. It is therefore important that the planning phase – the lead-in time before the participants even arrive to take part – is long enough to organize all elements necessary and anticipate any potential logistical issues.

It was stated repeatedly throughout this Report that having clear objectives is the most important aspect of that planning phase (Gomez, 2018; IAEA, n.d.). Everything about planning and staging an exercise stems from the goals the exercise is to achieve. The first step should be to establish clear and achievable goals. Another important aspect of planning to bear in mind is that the larger the exercise, the longer the planning phase needs to be. By way of example, *Cyber Europe 2016* was conducted 13-14 October 2016, but the planning began 12-13 May 2015, 18 months before the main exercise (ENISA, 2017, p. 11). *Cyber Europe 2016* was a successful multinational, multi-entity exercise which took place over only two days, but the scale of the enterprise and the logistics required to ensure that all the participants had a beneficial and useful experience was such that planning took exponentially longer.

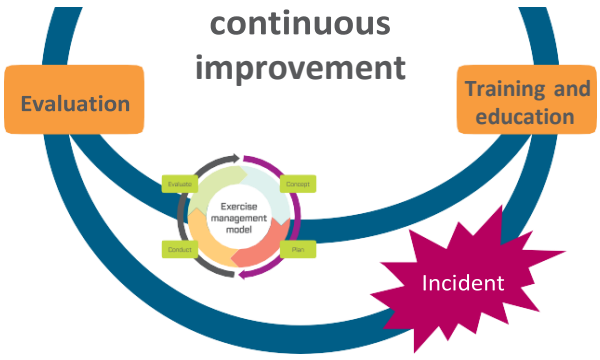
A final point to make on the planning of exercises is that preparation should not start by focusing on technical or technological aspects of exercises (Vykopal and Mokoš, 2016). Just as it is tempting for exercise organizers to opt for a full-scale simulation when such an exercise may not be appropriate for the learning outcomes, planning an exercise by focusing on technological features risks losing sight of more down-to-earth and realistic goals that may more accurately reflect a real-world situation.

To help with planning exercises there are aids in the literature. While not directly related to cyber security, the Australian Handbook on Disaster Management provides an excellent summary – a "planning circle" – which highlights the key milestones and goals (Australian Institute for Disaster Resilience, 2012, p. 15). This circle is provided in Diagram 1. These are intended to be used when planning a medium to large-scale exercise, but can easily be applied to small, single-entity activities.

The most important takeaway from this diagram is that conceptualizing and planning an exercise must work in concert with conducting the exercise (the actual staging of it) and a period of post-activity reflection or evaluation. In order for lessons to be learned, the experiences of all actors involved – organizers, participants and support staff – must be examined and taken into consideration. This is vital in order to identify lessons for future exercises, but also to identify the lessons that the exercise can teach about cyber security and defense *in the context of the exercise goals*. There is no benefit to conducting exercises merely for the sake of doing so. Whatever findings the exercises produce must go some way to informing policy and/or technical solutions. If this is done, then not only will the conduct of exercises be improved, but so too will preparedness in the event of an incident. Once again, the Australian Institute for Disaster Resilience provides a diagrammatic summary of this continuous relationship, including how exercise management fits in (See Diagram 2).

Diagram 1: Exercise Management Model (Australian Institute of Disaster Resilience, 2012, p. 2)

Diagram 2: Cycle of Continuous Improvement (Australian Institute of Disaster Resilience, 2012, p. 1)



A final point to make regarding planning, and in particular resources management, is that, while the particular types of resources needed for an exercise are an important consideration, more important is ensuring that there are adequate supplies of each resource, be

that staff, hardware, incidentals such as catering or computing power to manage a simulation. As discussed in Chapter 5.2, where resources were not adequate, including in terms of communication channels, the participants' experiences suffered as a result.

7.3 Have realistic scenarios

A point repeated in both the literature and interviews studies for this Report is that the scenarios for exercises must be realistic. A rule of thumb from the Czech exercises is that "less is more". There is no point bombarding exercise participants with dozens of highly sophisticated and highly damaging cyber weapons if this situation is not likely to occur in reality. Keeping the exercise as realistic as possible – and potentially as low-key as possible – will ensure that participants learn as much as possible about their real-world activities and their real-world options (IAEA, n.d.). This was also a lesson learned in the 2018 edition of the *Cyber 9/12 Challenge*. The original planned scenario called for the final stage of an escalating cyber crisis to be a mid-air collision of two passenger airlines as a result of a hack of European air traffic control systems (ATS). The organizers realized at the last moment that were this to occur in real life, the collision would have resulted in over 600 civilian deaths. The decision was made prior to the final activities of the exercise to make the scenario a near-miss on the runway. The reason for this last-minute change was that the objectives of the simulation were to challenge participants to develop policy solutions. Having a mid-air collision with hundreds of fatalities would have dramatically altered the conditions of the scenario away from policy development to crisis management. Were a hack of the ATS to occur and lead directly to civilian deaths, the political response would not be a simple matter of policy development.

Not only should the story behind the scenario be believable but there should also be scope for a natural evolution. The IAEA makes the point that a highly controlled simulation – where organizer White Teams have a great deal of control over the development of the scenario – runs the risk of those White Teams interfering with the exercise's progression (IAEA, n.d.). Responding to unexpected events should be part of an entity's preparedness and if the scenario in a situation is too rigidly controlled this can adversely affect a participant's ability to improvise. This requires organizers and their White Teams to be flexible enough to adapt as the exercise progresses but still have an eye on the overall objectives and therefore ensure the exercise as a whole remains on track (Haggman, 2018b).

The realism of an exercise scenario is also crucial from an active learning perspective. The more realistic and engaging the simulation, the more participants will engage with the exercise and the more they will learn. Haggman points out that a good scenario setup will encourage such active participation, and that those who engage the most actively are the ones who get the most out of it (Haggman, 2018b).

7.4 Cyber ranges not called for

Dedicated cyber ranges – where participants can test new devices and technologies in a secure environment – were conspicuous by their absence in the research for this Report. There was no widespread call for the development or construction of dedicated cyber ranges, beyond a historic mention of their use by the EDA (Röhrig, 2013). There are a number of reasons for this absence. Cyber ranges tend to be highly technical in nature with a focus on testing technological capabilities and resources. While this is an important aspect of national cyber defense and cyber security, not all exercise goals require such a technological focus. Full-scale simulations and table-top exercises may not need to focus on this kind of testing, but on examining the implications of their use in a wider environment. Having gathered together participants for a simulation, it is not always appropriate to use this gathering to test a technological solution, but rather to evaluate its deployment in as real a situation as possible. The goal is therefore to examine its wider applicability, and not necessarily its effectiveness

7.5 Don't conduct exercises simply for the sake of conducting exercises

The final point to make in this Report is one of introspection. Exercises can be and have been immensely useful tools, both for learning purposes but also for training, communication and drill. However, a theme running through this Report has been the need for a focus on goals. Planners of cyber exercises – and any entity wishing to conduct such exercises – should keep in mind the learning goals and not simply focus on staging more or larger exercises. Bigger is not always better. There is a danger that the actual and practical value of the exercises will be lost if there is a constant drive to increase the complexity of an exercise or its participant numbers (ENISA, 2015, p. 30). If a learning objective can be better and more effectively met with a small-scale exercise, do that rather than a full, resource-intensive simulation in which the smaller goals may become lost in the work of setting up and operating the simulation.

8 Bibliography

Australian Institute for Disaster Resilience, 2012. Handbook 3 Managing Exercises | Australian Disaster Resilience Knowledge Hub.

Baezner, M., In Press. 2017: Cyber Conflicts in Perspective - Hotspot Synthesis.

CCDCOE, 2013. Cyber Defence Exercise Locked Shields 2013 After Action Report. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

CCDCOE, 2012. Cyber Defence Exercise Locked Shields 2012 After Action Report. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

CCDCOE, 2010. Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Cederberg, A., 2018. Interview: Cyber Simulations as Education Tools.

Cordey, S., 2018. Finland, in: Dewar, R.S. (Ed.), National Cybersecurity and Cyberdefense Policy Snapshots, ETHZ Cyber Defense Project. ETH, Zurich, Switzerland.

Cyber Defense Magazine, 2018. Operation Eligible Receiver – The Birthplace of Cybersecurity: Configurations – Cyber Defense Magazine.

Department of Homeland Security, 2011. Cyber Storm III: After Action Report. US Department of Homeland Security, USA.

Department of Homeland Security, 2009. Cyber Storm II: After Action Report. US Department of Homeland Security, USA.

Department of Homeland Security, 2006. Cyber Storm I: After Action Report. US Department of Homeland Security, USA.

Dewar, R., 2014. The "Triptych of Cyber Security": A Classification of Active Cyber Defence, in: Prangetto, P., Maybaum, M., Stinissen, J. (Eds.), 6th International Conference on Cyber Conflict. NATO CCD COE Publications, pp. 7–22.

Dewar, R.S., 2018. The United Kingdom, in: Dewar, R.S. (Ed.), National Cybersecurity and Cyberdefense Policy Snapshots, ETHZ Cyber Defense Project. ETH, Zurich, Switzerland.

Egloff, F., 2018. Interview: Cyber Simulations as Education Tools.

ENISA, 2017. Cyber Europe 2016: After Action Report. European Network and Information Security Agency.

ENISA, 2015. The 2015 Report on National and International Cyber Security Exercises.

ENISA, 2012a. Cyber Europe 2012 - Key Findings Report. ENISA.

ENISA, 2012b. On National and International Cyber Security Exercises.

ENISA, 2011. Cyber Europe 2010: After Action Report. European Network and Information Security Agency.

GCSP, 2018. CYBER 9/12 STUDENT CHALLENGE 2018 [WWW Document]. URL https://www.gcsp.ch/Events/CYBER-9-12-STUDENT-CHALLENGE-2018 (accessed 8.11.18).

Gomez, M.A., 2018. Interview: Cyber Simulations as Education Tools.

Haggman, A., 2018a. The Great (Cyber) Game.

Haggman, A., 2018b. Interview: Cyber Simulations as Education Tools.

Hoffman, L.J., Rosenberg, T., Dodge, R., Ragsdale, D., 2005. Exploring a national cybersecurity exercise for universities. IEEE Secur. Priv. 3, 27–33.

IAEA, n.d. Module L-054: Scenario, Injects and Data.

IAEA, n.d. Module L-051: General Concepts of Exercises to Test Preparedness.

ISO, 2013. ISO 22398:2013 - Societal security -- Guidelines for exercises.

Jürgensen, N., 2017. Mehr als 20 Gigabyte Daten entwendet. Neue Zür. Ztg.

Krain, M., Shadle, C.J., 2006. Starving for Knowledge: An Active Learning Approach to Teaching About World Hunger. Int. Stud. Perspect. 7, 51–66. https://doi.org/10.1111/j.1528-3577.2006.00230.x

Kruger, D., 2012. Radically Simplifying Cybersecurity.

Martelle, M., 2018. Eligible Receiver 97: Seminal DOD Cyber Exercise Included Mock Terror Strikes and Hostage Simulations [WWW Document]. Natl. Secur. Arch. URL https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations (accessed 8.7.18).

Murphy, I., 2017. BT & Airbus set Cyber Security Challenge. Enterp. Times.

Prior, T., Roth, F., 2016. CSS Study: Learning from Disaster Events and Exercises in Civil protection Organizations (CSS Study), Risk and Resilience Reports. Center for Security Studies, Zurich.

Rapid7, 2017. Cybersecurity exercises – benefits and practical aspects. Rapid7 Blog.

Rid, T., 2013. Cyber War Will Not Take Place. Hurst, London.

Röhrig, W., 2013. Mainstreaming European Military Cyber Defence Training & Exercises.

RUAG, 2016. Cyber attack on RUAG: major damage averted [WWW Document]. URL https://www.ruag.com/en/news/cyber-attack-ruag-major-damage-averted (accessed 8.6.18).

Smith, E.T., Boyer, M.A., 1996. Designing in-class simulations. PS Polit. Sci. Polit. 29, 690–694.

Smith, R., 2010. The Long History of Gaming in Military Training. Simul. Gaming 41, 6–19. https://doi.org/10.1177/1046878109334330

Vegetius, 2001. Epitoma rei militaris: Epitome of Military Science, 3rd ed. Liverpool University Press.

Vykopal, J., Mokoš, O., 2016. Czech Cyber Defence Exercise: Lessons Learned.

Weitz, M.A., 1998. Drill, training, and the combat performance of the Civil War soldier: Dispelling the myth of the poor soldier, great fighter. J. Mil. Hist. 62, 263–289.

9 Appendices

9.1 List of acronyms and abbreviations used

Acronym	Full Phrase
AAR	After Action Report
ATS	Air traffic control systems
BOGSAT	Bunch Of Guys Sat Around a Table
CCDCOE	Co-operative Cyber Defense Center of Excellence
CERT	Computer Emergency Response Team
C-Suite	"Chief"-level directors or officers in a corporation, such as Chief Executive Officer (CEO), Chief Operations Officer (COO),
CtF	Capture-the-Flag; a form of war-gaming where participants are divided into red (attacking) and blue (defending) teams
EDA	European Defence Agency
ENISA	European Network and Information Security Agency
EU	European Union
GCSP	Geneva Centre for Security Policy
IAEA	International Atomic Energy Agency
ICT	Information and Communications Technology
ISO	International Organization for Standardization
NATO	North Atlantic Treaty Organization
Red-Teaming	Audit of an organization for compliance purposes or to measure that organization's level of preparedness
RUAG	**R**üstungs **U**nternehmen **A**ktien**g**esellschaft - Swiss defense technology firm
SME	Small and medium-sized enterprises

9.2. List of exercises examined

Name of Exercise	Date AAR published	Host	Scale
Baltic Cyber Shield	2010	• NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) • Swedish National Defence College (SNDC). • Swedish Defence Research Agency (FOI) • Estonian Cyber Defence League (ECDL) • Swedish Civil Contingencies Agency (MSB) • Swedish National Defence Radio Establishment (FRA) • NATO Communication and Information Systems Services Agency Computer Incident Response Capability - Technical Centre (NCSA NCIRC - TC)	Multinational
Cyber 9/12	Took place April 2018 but no AAR published	• Geneva Centre for Security Policy • Atlantic Council	Multinational
Cyber Czech 2014	2014	• Czech National Cyber Security Centre (NCSC)	Czech Republic
Cyber Europe 2010	2010	• European Network and Information Security Agency	EU
Cyber Europe 2012	2012	• European Network and Information Security Agency	EU
Cyber Europe 2014	2014	• European Network and Information Security Agency	EU
Cyber Europe 2016	2016	• European Network and Information Security Agency	EU

Cyber Storm I	September 2006	• US Department of Homeland Security National Cyber Security Division	Multinational
Cyber Storm II	July 2009	• US Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division	Multinational
Cyber Storm III	July 2011	• US Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division	Multinational
Cyber Storm IV	June 2015	• US Department of Homeland Security National Cybersecurity and Communications Integration Center	Multinational
Cyber Storm V	July 2016	• US Department of Homeland Security National Cybersecurity and Communications Integration Center	EU
Locked Shields 12	2012	• Swiss Armed Forces (SAF) Command Support Organisation • Finnish Defence Forces (FDF), • NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) • Estonian Cyber Defence League (ECDL)	Multinational
Locked Shields 13	2013	• NATO CCD COE • Estonian Defence Forces • Estonian Information Systems' Authority • Estonian Cyber Defence League • Finnish Defence Forces	Multinational

Locked Shields 14	2014	• NATO Cooperative Cyber Defence Centre of Excellence • Estonian Defence Forces • Estonian Information Systems Authority • Estonian Cyber Defence League • Finnish Defence Forces	Multinational
The Great (Cyber) Game	2018	• Andreas Haggman, Royal Holloway University of London	n.a.

9.3. Useful publications relating to the conduct of exercises

Document Title	Publisher
CSS Study: Learning from Disaster Events and Exercises in Civil Protection Organizations	Center for Security Studies, ETH Zurich
Exploring a national cybersecurity exercise for universities.	IEEE, Hoffman, L.J., Rosenberg, T., Dodge, R., Ragsdale, D.,
Handbook 3 Managing Exercises	Australian Institute for Disaster Resilience
ISO 22398:2013 - Societal security -- Guidelines for exercises	International Organization for Standards
Module L-051: General Concepts of Exercises to Test Preparedness	IAEA
Module L-054: Scenario, Injects and Data.	IAEA
On National and International Cyber Security Exercises	European Network and Information Security Agency
The 2015 Report on National and International Cyber Security Exercises.	European Network and Information Security Agency

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.