Preparing for National Cyber Crises Using Non-linear Cyber Exercises

Florian Skopik*, Maria Leitner†*
*AIT Austrian Institute of Technology, Center for Digital Safety & Security
firstname.lastname@ait.ac.at
†University of Vienna, Faculty of Computer Science
maria.leitner@univie.ac.at

***Abstract*—Cyber exercises are a well-received and established means to strengthen the problem-solving skills of personnel and to prepare staff for future cyber incidents. While this concept seems to work for the majority of expected issues, where practicing the application of specific processes, tools and methods to mitigate the effects of large-scale cyber attacks is key, existing cyber exercise approaches are just of limited use for crises management. The reason for this lies in the very nature of a crisis. While 'common' incidents appear to be more predictable and can usually be dealt with thoroughly prepared standard procedures and well-rehearsed responses, crises however, are inherently uncertain, and off-the-shelf solutions may even be counterproductive. Complex decisions are to be made in short time-frames, influenced by a lot more stakeholders compared to internal incidents, including regulators, the media, and even the general public. These decisions can barely be guided by prepared plans or checklists, thus new forms of preparation are required, which challenge the participants to practice decision making under pressure, but further give them the opportunity to re-consider choices, walk alternative paths and enable them to find the best possible solution for a given situation. For this purpose, this paper discusses a new approach for non-linear cyber exercises, which allow *branching points* to develop a storyline, and employ new techniques, such as '*Fast Forward*' to quickly progress to the critical stages of long-lasting crises, '*Playback*' to consolidate gained skills, and '*Pause-Adapt-Repeat*' to play through alternative paths. In this paper, we discuss limiting factors of today's cyber exercises for large-scale cyber crises preparation, and introduce concepts for non-linear exercises to compensate these issues.**

***Index Terms*—cyber crisis, crisis management, national coordination, cyber crisis preparation, exercise platform, non-linear games**

I. Introduction

Cyber Europe, Locked Shields, and Cyber Coalition are just some popular examples of today's wide landscape of international cyber security exercises [1], [2]. These exercises are massive and meant to provide a vital means to prepare and test personnel of national cyber security centers, national CERTs and authorities for professionally challenging and personally stressful situations following a large-scale nation-wide cyber attack or incident. In recent years the number of organized cyber exercises has grown exponentially [1]. Although they require a tremendous amount of preparation at the organizers' side and are immensely cost-intensive, they are nevertheless a foundational pillar of most national cyber security strategies [3].

The basic idea of cyber exercises is that in a simulated environment personnel tries to solve serious issues in an open or guided manner to test their problem solving cyber capabilities and prepare for real incidents, should they happen anywhere in the future. While this concept seems to work for the majority of expected issues, where practicing the application of specific processes, tools and methods to mitigate the effects of large-scale cyber attacks is key, we argue that it is just of limited use for "national cyber crises management" (CCM) [4]. The reason for this lies in the very nature of a crisis. A crisis is commonly defined [5] as "an abnormal and unstable situation that threatens an organization's strategic objectives, reputation or viability." However, this is just half of the truth for cyber crises. Additionally, and in contrast to 'common' crises, the time critical call for action and the extraordinary management efforts in response is even more critical in context of a cyber crisis.

While common incidents appear to be more predictable (i.e., something that happens regularly and follows thought-through paths) and can be addressed with predefined and well-rehearsed responses, crises however, are inherently uncertain, and not manageable with off-the-shelf solutions. For example, if numerous, even independent incidents occur simultaneously (as it can be expected at the national level), they may develop into a crisis if the planned response do not work out as expected, or if the concerned organizations are not able to recover. Therefore, we argue that dealing with crises demands more flexible and creative thinking than incidents – and thus call for new forms of preparation, different from common cyber exercises.

Incidents have serious, but usually lesser impacts than crises. A crisis may however may arise from incidents which were not properly resolved. Poor responses, specifically, poor management and decision making due to uncertainties while handling a crisis can be fatal for organizations and businesses; and this is even more true for a whole nation state. A critical question therefore is, how to appropriately prepare for these unknown situations.

As a prerequisite a few very important issues need to be addressed. Therefore, the contributions of this paper are:

- **Cyber crises:** We shed light on factors that facilitate the emergence of cyber crises and outline possible future situations that can lead to national cyber crises.

- **Limiting factors of cyber exercises:** With respect to the factors that might lead to cyber crises, we survey the specific requirements for a CCM exercise approach.
- **Approach for CCM exercises** We discuss a new approach for non-linear cyber exercises, which allow branching points to develop a storyline, and employ new techniques, that satisfy specifically the requirements of cyber crises management.

The remainder of the paper is organized as follows. Section II outlines the factors that facilitate the emergence of crises, and outlines possible future scenarios that might evolve into crises. Section III critically reviews the feasibility of established cyber exercises to prepare for crises situations and summarizes specific requirements on a new CCM exercise approach. In Sect. IV, we outline the methodology of a new approach and its foundational pillars, and discuss its applicability. Finally, Sect. V concludes the paper.

II. Background and Related Work

Crisis emerge from unforeseen issues, specifically when the carefully designed contingency measures do not apply well enough and an otherwise controlled incident solving process gets out of control. The challenge with crises management is that it is not possible to come up with elaborated response plans in advance. It is also not easy to train for crises, since no one can properly plan for the unforeseen. There is a multitude of factors that might contribute to the emergence of a crises. In this paper, we aim for a structural analysis of these factors through reviewing previous cyber incidents.

A. On the emergence of cyber crises

The evolution from a large-scale incident to a cyber crises is a subtle one. After intense research of previous cyber incidents and their treatment [6]–[8] and backed up by [9], we infer that a large-scale high-impact incident becomes a crises if it escapes from the expected script, i.e., if something in the processing of the incident goes wrong or behaves unexpectedly. Based on the literature review, this might be the case with:

- **New technologies.** Incidents concern new or broadly unknown technologies or domains, where the impact was not anticipated realistically, e.g., large-scale IoT networks [10].
- **Communication breakdown.** The line of communication with the crisis management group is interrupted or not reliable any longer due to parallel incidents that concern the availability of technology or people.
- **Insider threat.** There is a threat from the inside which destroys trust in the communication with and decisions of the crises management team.
- **Lack of expertise.** Required expertise is not obvious or not available. Who to involve and who to inform is based on guesses at best.
- **External dependencies.** Problems can only be solved with external help (e.g., from neighboring countries, industry associations etc.), however, these dependencies cannot be satisfied.
- **Long-running incidents.** The incident lasts for days, spanning multiple shifts of people which makes the handover challenging. In this time, the improper handling lets the incident emerge to a crises.
- **Resource shortfall.** Only a few people have the expertise to analyze complex attacks – and these people are not available 24/7. A challenging technical issue paired with a pandemic crisis further tenses a situation.
- **Cascading effects.** There are unforeseen cascading effects or unprecedented long-term impact.

B. An overview of potential cyber crises scenarios

On an organizational level, multiple definitions of cyber crisis exist in the literature, although they all have in common that a crisis refers to more serious incidents that may either cause significant financial loss or brand reputation damage, or fundamentally threaten the survival of the organization (or even both) [9]. Furthermore, in contrast to (small-scale technical) cyber incidents, senior management must always be involved.

On a national level [11], it is however even harder to come up with a consistent definition of cyber crisis. For instance, Israel defines it this way: ”A cyber crisis is liable to cause real damage and disrupt functional continuity, and to escalate to the point of a national state of emergency.” [12]

Looking at the cyber incidents of recent years, we argue that real cyber crises at the national level are rare. Despite many incidents may have high financial impact to a single organization, but in most cases no long-lasting effect on the population can be observed. Nevertheless, a series of incidents may lead to severe impact on a nation state and justify a crisis situation, such as:

- Compromised root certificates of large certificate authorities and thus no trustworthy Internet communication.
- A compromised firmware or implanted backdoors in core Internet infrastructure, such as core routers, DNS servers and the like.
- A severe vulnerability in a widely used library that can neither be easily fixed nor replaced.
- Long-Lasting disruption of essential cloud services or content delivery networks.
- Compromised financial services across the whole financial sector.
- Mass Denial-of-Service attacks that cannot be treated by ISPs and scrubbing centers.
- Weaknesses in national electronic identity services.
- Misuse of widely deployed technology on a large-scale, such as hacking of autonomous cars, smart home devices and the like.
- Successful espionage attacks to national and governmental institutions.
- Distribution of deep fakes that cause mass panic.

Table I
TYPICAL SIMPLIFICATIONS IN TODAY'S EXERCISES.

id	simplified aspect	description
S1	training baseline	Often trainings are based on previous incidents and/or thought-trough scenarios from risk assessments only and do not anticipate future (technological) developments, e.g., exercise something completely new.
S2	artificial line of communication	The line of communication and escalation is often simplified and artificial since the scope of the exercise is limited in nature.
S3	staff scope	The group of involved persons and roles are well defined in advance; there is no need to think about who to involve, to approach, or to report to during an exercise because of its limited scope in terms of staff members.
S4	Kobayashi Maru	Exercises usually provide a 'solvable' problem. Participants know that they have got everything they need (tools, knowledge, personnel) to solve a situation. There is no need to questions the own capabilities.
S5	limited time-span	Most exercises play through the complete life-cycle of a problem, which is solvable within a work day (the scheduled training time). Fatigue or shift changes are barely considered.
S6	distribution of team members	Often all participants are co-located which makes communication, availability, and reachability impossible to train and simplifies the situation.
S7	clear organizational boundaries	The organizational units, which participate in the exercise, are in scope, everyone else is usually out of scope. Questions concerning who to involve or who to escalate to are therefore predetermined. Responsibilities are immediately obvious.
S8	external contacts	The exchange with external entities is often simulated poorly, e.g., the involvement in authority processes in case of crime investigations or reported breaches. For exercises this may be fine from an organizational point of view, but not from a national perspective.
S9	technology scope	The affected technology is predetermined by the scenario and required expert knowledge is in line with the participants' expertise.
S10	training of existing solutions	The goal for participants is to train the application of their specific tool-sets and processes to strengthen their handling capabilities. 'Out of the box' thinking is usually not required.
S11	artificial operations	Several operational aspects are usually artificial, since certain tools and processes are required for the exercise and provided by the host organization but not present in the real world, e.g., tools to observe and rate the participants' behavior and actions.
S12	clear threat model	To the best of our knowledge, mostly external threat actors are assumed. Real-world concerns, such as internal enemies and distrust among the cooperating partners is out of scope of most exercises.
S13	availability	Missing personnel and resources, fatigue, holiday and general unavailability of key personal is no issue in most exercises. Even worse, most exercises are planned in a way that first-choice key personnel is available.

III. LIMITATIONS OF CYBER EXERCISES

We take a closer look into common simplifications of cyber exercises and derive some high-level requirements on an exercise methodology that are supposed to compensate their negative effects.

A. *Simplifying factors and assumptions of cyber exercises*

The realism of every exercise suffers from inherent simplifications and assumptions that are made in order to ease the delivery of the exercise. After investigating a wide range of cyber exercises and conducting interviews with cyber security experts from national bodies and the military domain, several factors were identified as listed in Table I.

We argue that these assumptions and simplifications are mostly fine for exercises with limited scope, since every exercise tries to train a certain aspect (e.g., the use of technology/tools, application of know-how, practicing communication and reporting etc.). However, staff in crises management is often simultaneously challenged with all of these aspects.

Thus, as outlined before, the nature of a cyber crisis lies in the fact that many disadvantageous factors combine in a unique and unforeseen manner – something which can hardly be trained in a simplified setting.

B. *Requirements on an exercise methodology*

In order to address and compensate the aforementioned simplifications, we derive a set of mandatory high-level requirements on an exercise methodology. The methodology must allow to:

- Requ-1: create a serious crisis situation through the combination of multiple incidents and deliver them in parallel (addresses S1, S2, S4, S7),
- Requ-2: simulate change of shifts through jumping forward in the storyline (addresses S5, S13),
- Requ-3: allow the participants to reflect on unexpected events (addresses S1, S7, S8, S10),
- Requ-4: include and simulate external players, such as national authorities, regulators or vendors (addresses S2, S3, S8, S11),
- Requ-5: allow participants to exercise in a distributed setting (addresses S2, S7, S11, S13).

IV. NON-LINEAR CYBER EXERCISES

In order to overcome the stated limitations (cf. Table I) and fulfill the requirements derived before, we extend a common exercise methodology with novel non-linear elements.

A. *Basic concept and model*

The basic elements include many of the well-known cyber exercise elements [13], including:

- **Players and non-player characters**, i.e., besides the actual participants, several real or simulated persons are required to progress through the story, such as decision making outside the exercise scope.
- **Injects via simulated interactions** are the means to control the pacing of the exercise. An inject is simply any kind of event that is communicated to the participants.
- **Several complex scenarios in parallel** allow the escalation of otherwise treatable incidents into crises. Overlapping story elements, such as a problem that spreads across an infrastructure, help to maintain a realistic story compared to completely unrelated occurrences of problems.

We foresee each exercise story separated into different phases that correspond with the common phases of crises management, i.e., its emergence, analysis, containment and resolution [9]. Certain phases may force participants to act under stress, others require certain professional expertise or experience. However, break points are an integral means of the delivery approach, where the exercise is paused and decision of participants revisited/discussed and even revised (see below). Besides that, "unusual influencing factors" (e.g., simulated shifts, broken toolchains, ...) that have the potential to let serious incidents evolve to real crises are an essential part of proper cyber crises exercises.

B. Non-Linear exercise elements

The cyber scenario is primarily based on the storylines of a script. In doing so, the framework conditions, the initial situation and the possible effects on the participating organizations, but also on the interested parties, are already specified. In a 'classic' exercise participants receive a series of *injects* that constitute *incidents*. Several incidents make up a *story*. While incidents are situations or events within the scope of the storylines, which further detail them and often serve as a point of reference for the exercise management, injects are the actual information delivered step-by-step to the exercise participants. Usually, injects are specifically developed for the respective exercise participants in the cyber scenario. The order and timeframe of inject delivery is usually strictly linear and pre-scripted (cf. Fig. 1). [13]

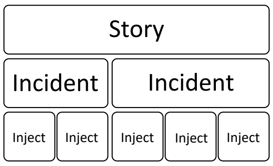

Figure 1. The foundational elements of cyber exercises.

In a non-linear exercise, however, we provide the following functions additionally to timed and pre-scripted inject delivery:

- **Forking:** We work out different alterations of the same story in advance, e.g., a spreading malware that progresses with different speeds. At specific points in the story, participants are asked to make explicit decisions, e.g., on mitigation measures, and the exercise control decides which story line to carry on.
- **Fast-Forward:** Incidents whose treatment has been trained already in the past, but which are important for the story can be skipped or played through with elevated speed. This is specifically important for long lasting cyber crises to progress to the later stages of crises management without the need to run the exercise for days. So, some sections of the story line which may take hours to play though can be compressed into minute or completely jumped over by using pre-scripted responses to the respective injects.
- **Playback:** This mechanism allows the player to rewind the story, got back to a previous point and treat a number of incidents again. This requires the exercise platform [14] to reset the story to a previous state. The reason for that is to give participants the chance to take a closer look into what information was available at a previous certain point in time and to reconsider decisions. Specifically, this mechanisms is not meant to influence the outcome of incident response, but merely to halt the exercise and trigger off discussions.

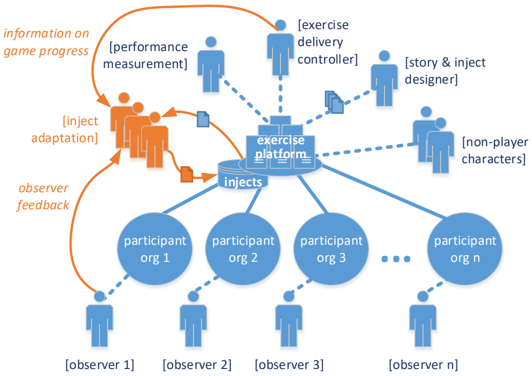

Figure 2. The basic roles in the delivery of a cyber exercise, extended by [inject adaptation] (in orange).

- **Pause-Adapt-Repeat:** Reflection on executed actions may let participants reconsider their choices. So, with this function, they may go back in time, adapt their decisions, and repeat the treatment of the last few injects. This mechanism could further be used by the exercise management to adapt a scenario, should participants be overwhelmed or should they have taken a path which hinders the further smooth delivery of the exercise.

C. Planning and delivery

Figure 2 visualizes the minimum setup for delivering cyber exercises. A [story and inject designer] prepares the injects to lead the participants through the pre-scripted story. An [exercise delivery controller] ensures the smooth and timely delivery of injects to participants. Several [non-player characters] simulate responses from persons outside of the exercise scope. The role [performance measurement] keeps track of the exercise delivery and participants' progress. One or several [observers] collect impressions from the participants. With this minimum setting, a common linear exercise can already be delivered.

We extend this common setup with a new role: [inject adaptation]. A story is basically pre-scripted and provides for expected reactions from the participating organizations. If these deviate from these expectations, experts have to react to a changed cyber situation. For this purpose, new framework conditions in the form of injects and / or stage directions usually have to be developed in situ. One or several people collect feedback of the participants' progress from the [exercise delivery controller] as well as from [observers] and adapt pre-scripted injects accordingly on the fly. The collection of both feedback from the controller as well as from observers is essential to appropriately rate the participants' status and steer the inject adaptation. For instance, while participants

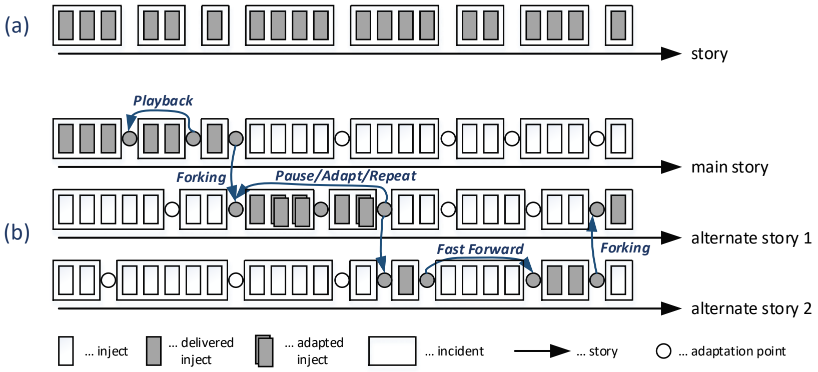

Figure 3. The delivery of injects (a) using the linear classic model, and (b) using adaptation points to achieve non-linearity.

may progress just fine on the exercise platform [14], an observer could spot deviations from expected role behavior or uncertainties of participants that justify the repeated delivery of some parts of the story.

Figure 3 shows the types of adaptations that may take place. Some decision of participants may let them switch to alternate story lines (*Forks*) to better reflect the consequences of their actions. Complex responses to injects may be retrained by delivering them multiple times in loops (*Playback*) or with potential modifications (*Pause/Adapt/Repeat*), while injects that lead to well-known situations or that do not deliver any positive training effect, can effectively be run through with higher speed (*Fast Forward*).

Notice, since an exercise always involves a part of simulation, queries from participants to ”external third parties” who are not actively involved in the cyber exercise must be answered or processed by non-player characters. To this end, it is important to agree a communication process with the participants in advance, which ensures that no undesired communication with external third parties is initiated.

V. Conclusion and Future Work

This paper described common simplifications of cyber exercises and argued why these are problematic in context of cyber crises exercises. We proposed a non-linear exercise delivery model, which is meant to simulate the uncertainties of cyber crises in a more realistic manner. Furthermore, points of discussion and reflection for participants are an integral part of such trainings.

Training for cyber crises is different from training for well pre-scripted cyber incidents. While many exercises focus on training of specific processes or the handling of technologies, cyber crises strongly demand – due to their inherent uncertainties – self-organization skills, critical thinking, stress resistance, communication skills and leadership. Future work therefore deals with the question to what degree these capabilities can actually be trained and how much they must be gained through experience. For that purpose, this training methodology will further be applied together with national stakeholders in the field of cyber security, including sectoral CERTs and ministries, in course of a running research project.

Acknowledgment

This work was partly funded by the FFG project CADSP (873425).

References

[1] A. Ogee, R. Gavrila, P. Trimintztos, V. Stravropoulos, and A. Zacharis, “The 2015 report on national and international cyber security exercises - survey, analysis and recommendations,” 2015. [Online]. Available: https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

[2] E. Seker and H. H. Ozbenli, “The concept of cyber defence exercises (cdx): Planning, execution, evaluation,” in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 2018, pp. 1–9.

[3] H. Luiijf, K. Besseling, M. Spoelstra, and P. De Graaf, “Ten national cyber security strategies: A comparison,” in *International Workshop on Critical Information Infrastructures Security*. Springer, 2011, pp. 1–17.

[4] S. Boeke, “National cyber crisis management: Different european approaches,” *Governance*, vol. 31, no. 3, pp. 449–464, 2018.

[5] BSi, “Bs 11200: 2014: Crisis management. guidance and good practice,” 2014.

[6] M. N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z. Z. Abidin, N. S. Ali, and K. H. Abdulkareem, “Cyber-security incidents: a review cases in cyber-physical systems,” *Int. J. Adv. Comput. Sci. Appl*, no. 1, pp. 499–508, 2018.

[7] F. Skopik, *Collaborative cyber threat intelligence: detecting and responding to advanced cyber attacks at the national level*. CRC Press, 2017.

[8] F. Skopik, G. Settanni, and R. Fiedler, “A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing,” *Computers & Security*, vol. 60, pp. 154–176, 2016.

[9] P. Trimintzios, R. Holfeldt, M. Koraeus, B. Uckan, R. Gavrila, and G. Makrodimitris, “Report on cyber crisis cooperation and management,” 2014.

[10] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, “Understanding the mirai botnet,” in *26th USENIX security symposium*, 2017, pp. 1093–1110.

[11] F. Skopik, Z. Ma, P. Smith, and T. Bleier, “Designing a cyber attack information system for national situational awareness,” in *Future Security Research Conference*. Springer, 2012, pp. 277–288.

[12] Cyber Israel, “National cyber concept for crisis preparedness and management,” 2018. [Online]. Available: https://www.gov.il/BlobFolder/news/cybercrisispreparedness/en/Management%20of%20crisis%20situations%20english%20final.pdf

[13] J. Kick, “Cyber exercise playbook,” MITRE CORP BEDFORD MA, Tech. Rep., 2014.

[14] M. Leitner, M. Frank, W. Hotwagner, G. Langner, O. Maurhart, T. Pahi, L. Reuter, F. Skopik, P. Smith, and M. Warum, “Ait cyber range: flexible cyber security environment for exercises, training and research,” in *Proceedings of the European Interdisciplinary Cybersecurity Conference*, 2020, pp. 1–6.