TRANSFERRING THE CONCEPT OF TABLETOP EXERCISES INTO THE LEGAL DOMAIN

Peter Kieseberg / Simon Tjoa / Melisa Gafic

Peter Kieseberg, Senior Researcher, UAS (FH) St. Pölten, Institute of IT Security Research
Campus-Platz 1, 3100 St. Pölten, AT
Peter.Kieseberg@fhstp.ac.at; https://www.fhstp.ac.at/de

Simon Tjoa, Professor and Head of Department, UAS (FH) St. Pölten, Department of Computer Science and Security
Campus-Platz 1, 3100 St. Pölten, AT
Simon.Tjoa@fhstp.ac.at; https://www.fhstp.ac.at/de

Melisa Gafic, Researcher, UAS (FH) St. Pölten, Department of Computer Science and Security
Campus-Platz 1, 3100 St. Pölten, AT
Melisa.Gafic@fhstp.ac.at; https://www.fhstp.ac.at/de

Schlagworte: ***Cyber Security, Exercises, Simulation Games, Legal Incident Handling***

Abstract: *The strategy of simulating cyber incidents and training their subsequent handling is gaining increasing importance, as hands-on exercises are seen to be a vital part in developing practical skills under stress and external influences. Thus, on a technical level, these exercises have reached a good level of professionalism. Still, typical scenarios focus on the technical aspects, while legal issues are only considered as sub-topic at the side. With respect to the rising importance of legal matters in IT, this needs to be addressed. In this work we discuss, how use the method of conducting cyber exercises for training the legal aspects of cyber incidents.*

1. Introduction

Regularly practicing and testing cybersecurity plans is crucial for building successful security measures in an organization. Moreover, implementing a plan, even in a controlled (test) setting, helps revealing concealed misunderstandings and deficiencies, thereby facilitating the development of plans and policies that accurately represent the actual state of the company and work under the given circumstances. Furthermore, plans that undergo regular testing will be more readily adjustable in the event of alterations, such as modifications to the organizational framework or technical complications. However, the primary advantage of regular exercises is to familiarize individuals with the strategy and enable them to perform effectively under the pressure caused by attacks. These inherently instills confidence and establishes professionalism, both of which are crucial components for dealing with a real-life incident.

In IT, cyber exercises are currently typically focused on technical or managerial cyber security staff, ranging from very technical exercises where technical skills are evaluated and honed to purely communication related scenarios, where all technical aspects are simulated and the execution of contingency plans, as well as the inclusion of external experts, vendors, customers and higher management is the key target. In this area, the legal side of cyber incidents is regularly introduced into technical scenarios, still, this is typically done as a side show, i.e. the main focus remains on the technical solution of technical issues with some additional inclusion of the legal department. Often, the latter is not even in the role of a player, but rather a non-player character (NPC) and assumed into an expert role, i.e. the target of the scenario does not lay on solving a legal issue, as this is taken for granted, but in the technical managers introducing the legal department on time and in the right way.

Still, with the plethora of new tech-related legal documents, laws, regulations and best practices, put into place, providing a standard solution in the realm of law is not straightforward and needs to trainingtoo. This especially holds true in case of organizations applying artificial intelligence, as new legal requirements based on the AI Act[1] and related regulations add new and complex questions, especially in combination with other acts like DORA[2] or the GDPR[3]. Furthermore, these new regulations introduce (i) potentially high penalties in case they are violated and (ii) timely pressure, as issues need to be solved very fast. This results in scenario, where complex legal issues touching the realm of cutting-edge technologies need to be tackled in a very limited timeframe and under pressure.

In this paper, we focus on the adaption of tabletop cyber exercises[4] for legal matters in cyber incident management, i.e. instead of legal issues as a side matter to a technical focus, we put the focus on the legal questions with the technical reasons being background information only. Since cyber exercises aim at putting the players under pressure, this tool will be very helpful for training legal security experts for tackling real-life scenarios.

The paper is structured as follows: Section 2 gives background information on tabletop exercises in the cyber domain and the current inclusion of legal matters, Section 3 provides the approach for setting up tabletop exercises with a legal focus, while Section 4 concludes the paper and gives an outlook on future work in this direction.

2. Background & Related Work

In this section we provide an overview on the most important types of exercises, as well as an outline on the typical introduction of legal matters in these exercises. This section not only builds on academic literature in this field, but also on our extensive experience in conducting these exercises.

2.1. Cyber Exercises

Cyber exercises can be categorized into numerous types, typically depending on the specific technological level that the activity focuses on. Common implementations vary from intricate low-level exercises involving technical experts combating a technical attack to exercise scenarios focused solely on communication, where the technical aspect is simulated to practice decision-making and communication skills. Exercises must be customized to suit the specific needs and requirements of the organization(s) engaged, as well as the environment in which the organization(s) operate. Multi-organizational exercises pose significant complexity, as the allocation of necessary resources might be problematic. This complexity is even increased in case of international exercises, where different players have to follow different legal and governmental rules. In cross-organizational exercises, it is crucial to analyse issues related to information sharing among partners in advance, in collaboration with legal departments. This analysis should focus on determining the legality of sharing information within the framework of laws and regulations, such as the GDPR, which may pose challenges like e.g. the sharing of IP addresses. Additionally, it is important to assess whether strategic information is being shared with potential competitors, such as divulging contingency plan details that could provide unwanted insights to partners.

[1] Proposal for Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, COM/2021/206 final.

[2] European Commission 2020. Proposal for a regulation of the European Parliament on digital operational resilience for the financial sector and amending Regulations.(DORA).

[3] European Union: Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 (2016).

[4] See Ottis, R., 2014. Light weight tabletop exercise for cybersecurity education. Journal of Homeland Security and Emergency Management, 11(4), pp.579-592.

With respect to the cyber domain, the following types of exercises are frequently encountered:

- **Card and board games** are increasingly being used to experience ideas and concepts as well as decision-making situations in a playful way[5]. Various board games and game content have been developed for this purpose having been realised both online and offline.
- **Capture the flag (CTF)** is a computer security competition with challenging exercises from different categories (e.g. network security, application security, mobile security, etc.)[6]. Typically, the goal of the game is to find one or more flags, i.e. usually a flag is the solution to the given problem and can be found or solved through one or more steps or tasks within an exercise. A flag can, for example, be a string, an image or another element. Within the literature, there are several CTF games or challenge types:
  - ***Quizzes*** typically consist of a question-and-answer pair on computer security or related topics.
  - ***Jeopardy*** is a sequence of challenges or tasks that require participants‘ computer networking knowledge and skills. The aim of the participants is to solve these tasks to obtain the flag.
  - ***Attack-Defence*** games support offensive and defensive hacking between teams, i.e. teams are actually working against each other. Standard ***Red-Team-Blue-Team*** scenarios have distinctive attacker and defender teams, typically akin to actual roles in the respective organizations for the defender, while the attacker side is played by either other players or by specifically hired teams. Other mode, like classical ***Capture-the Flag*** have all teams in offense, as well as defence, with each team required to protect their “base” and conquer targets.
  - ***Mixtures*** are usually a combination of threat and attack defence CTF.
  - ***King of the Hill*** mode is about capturing and capturing a target system to keep it under control for as long as possible. A „King of the Hill“ challenge is characterised by a vulnerable system that is taken over.
- ***Cyber Ranges***, large technical game infrastructures used for the realization of technical cyber exercises in order to simulate the realism and dynamics of a real environment[7]. These infrastructures are typically purely virtual and can be customized to simulate various technical scenarios.
- ***Tabletop Exercises*** simulate an incident and, to a certain extent, the resolution[8]. This is typically done in the form of a management simulation, i.e. the technical details of the simulation are not really implemented but provided in a more or less artificial form. This allows for the integration of technical, as well as management staff. More details can be found in the following subsection.

2.2. Tabletop exercises

As outlined before, tabletop exercises simulate an incident, typically set completely apart from any real technical simulation, i.e. typically, there is no system set up, like in the case of a cyber range or a red-team-blue-team exercise, but organizations pretend that incidents happen in their actual infrastructure[9]. Of course, since this would cause too many unwanted side-effects, there is as little actual interference with these systems as possible, and the technical solution finding is purely simulated on a decision-making level. This kind of

[5] Nagarajan/Allbeck/Sood/Janssen, Exploring game design for cybersecurity training. 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 256-262. IEEE, 2012.

[6] Kucek/Leitner, An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. Journal of Network and Computer Applications, 151. 2020.

[7] Ecso. Understanding Cyber Ranges: From Hype to Reality (S. 31) [WG5 PAPER]. https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf : s.n., 2020.

[8] Ottis, Light weight tabletop exercise for cybersecurity education. Journal of Homeland Security and Emergency Management, 11(4), pp.579-592, 2014.

[9] Ottis, Light weight tabletop exercise for cybersecurity education. Journal of Homeland Security and Emergency Management, 11(4), pp.579-592, 2014.

exercise is especially suitable for simulating actual attacks against an infrastructure and especially the organizational and operational detection and reaction to it. Consequently, we need to outline a set of important definitions that we will refer to in the course of the paper[10], as they are essential for setting up tabletop exercises for legal cyber incident handling.

The term **Players Characters** or **Players** (short: **PCs**) is reserved for any participant in the exercise that plays his or her actual role in real life, of course with some deviation from reality due to simulation artificialities and is in the role of a protagonist in the scenario. In short, these are the persons the simulation is centred around and that are “exercised on” or trained. This also means, that they are not under the control of the exercise management and do not know about the scenario. Of course, tabletop exercises can also be used to get a feel for a new position, but still, the position the player needs to take over needs to be a real position with

All other entities are summarized under the term **Non-Player Characters (NPCs)**, these can either be persons playing their real role in life, or so-called simulators that take on one or various roles throughout the simulation. Typically, these NPCs are “in” on the scenario and receive information and reaction guidelines by the exercise management, i.e. they are under the control of the exercise management to a certain extent. In case of playing their real role, these NPCs are typically other entities in the company, or very important external entities. This role is typically reserved for e.g. the legal departments in most technical simulations. While these persons still work according to their normal behaviour, simulators are used to embody any other entity. This not only includes pre-planned personas that are foreseen in the scenario or logical contact points for the players, but also wildcards and persons/entities previously unknown to the exercise management. Taking on such a role can therefore become quite complex.

Exercise management[11] takes over the organization of the tabletop exercise, starting with finding dates and office space, providing the scenario, organizing the people required to attend the exercise and all other required organizational tasks. Most importantly, exercise management runs the simulation, i.e. it provides information to the player characters through so-called **injects**, information particles sent to them through various real and simulated means, they instruct the NPCs and (often ad-hoc) the simulators and steer the whole process by taking decision influencing the scenario and reacting got player actions. Exercise management is therefore largely responsible for the result and the value of the exercise and requires extensive preparation and a good portion of experience. They also are responsible for timekeeping and bringing the exercise to a fruitful and positive end.

The **scenario** is the basic story line of the simulation, i.e. the kind(s) of incident(s) that are played, planned obstructions and additional hurdles, as well as the planned exercise conclusion. Of course, the scenario will change during exercise execution due to the actions taken by the players, but well-planned exercises typically plan several paths for the most likely decisions. The scenario is typically split into phases in order to structure the simulation, starting with a setup phase, where the players get accustomed to the simulated inject.-based training environment, that typically differs a lot from their normal environments, as well as other exercise artificialities. In the detection phase, the players should find out that something is going wrong and what it is. In the escalation phase, the stress level is increased by the looming danger of (extreme) potential damage or repercussions. The target in this phase is solving the issue(s) at hand until the scenario reaches the solution phase, where the players need to apply the found solution. In the final phase, the remedy phase, everything goes back to normal. This structure also provides for a controllable story arch and gives the exercise management ample options for increasing or decreasing the stress level for the PCs. The basic scenario is typically

[10] See also Kaundert/Ziegler/Pahi/Skopik/Leitner/Kieseberg/Schwanzer/Ampia-Addison. Evaluierung des Cyber Lagebildkonzepts im praktischen Einsatz. Cyber Situational Awareness in Public-Private-Partnerships: Organisationsübergreifende Cyber-Sicherheitsvorfälle effektiv bewältigen (2018): 293-344.

[11] Gafic/Tjoa/Kieseberg/Hellwig/Quirchmayr, Cyber Exercises in Computer Science Education. In ICISSP (pp. 404-411), 2022.

one of the very first aspects of an exercise that is fixed, as it has great impact on further planning, like PCs and NPCs required, size and timing of the exercise.

Injects, as already mentioned in the paragraph related to exercise management, serve as means to drive the whole simulation and for informing the PCs on, what is actually happening. Since in a tabletop exercise, the incidents are not real but purely simulated, the PCs cannot resort to analysing their real systems, but must be told that something has happened, e.g. on their network. These injects not only convey technical information, about any information provided to the players apart from (simulated) direct communication. Injects can also be optional, e.g. in order to steer players that follow a wrong direction, in order to speed up or slow down the exercise or provide optional additional information. Furthermore, good exercise management is able to provide ad-hoc injects in case of a derailing exercise execution in order to bring it back on tracks.

2.3. Current inclusion of legal topics

While cyber exercises started out focusing on technical issues, especially when considering Red-Team/Blue-Team exercises, throughout recent years exercise scenarios started to increasingly focus on prominent and important issues regarding cybercrime, most notably ransomware cases[12]. Here, the role of the legal department is typically reduced to a pure information and abstract decision-making entity, i.e. the technical players are told by the legal department, played as an NPC by the organizers, how to proceed and whether the ransom will be paid or not. In these cases, the legal department is not actually conducting a legal analysis and also does not simulate contacting the respective authorities, but merely serves as a contact point and information drop for technical players.

Other exercises incorporate the legal department as players, but only in minor roles, e.g. deciding on the legality of countermeasures and actions taken by the technical departments or playing a small role with respect to compliance with certain regulations. Still, this kind of analysis does not lie at the hearts of these simulations, thus only playing a minor role in the whole scenario with a very limited timeframe attached to it.

3. Adapting cyber tabletop exercises for legal topics

In this section, we will provide our approach on adopting cyber exercises for focusing on legal topics around cyber incidents. It must be noted that every exercise is different, and many aspects not only depend on the scenario played, but especially on the target of the exercise with respect to individual training interests. Thus, we are only able to give suggestions and outlines, but not a comprehensive overview on every possible scenario and aspect. This also holds true for the exercise artificialities, as their individual impact also largely depends on the individual exercise setting.

3.1. Possible Use-Cases and Scenarios

Exercising the legal implications of cyber incidents is currently underdeveloped and often seen as a side topic in exercises focusing on technical aspects of cyber security. Thus, in this section we outline four types of use cases and scenarios that are of high importance now or in the near future.

Dealing with cybercrime: This is the most straightforward scenario where legal issues play a vital role and are typically often only delt with as side issues in technical exercises. The very prominent issue of ransomware, especially in combination with extortion or even selling the data afterwards to a competitor (so-called triple extortion attacks) introduces a lot of legal questions with respect to internal/external rules and legal

[12] Kaundert/Ziegler/Pahi/Skopik/Leitner/Kieseberg/Schwanzer/Ampia-Addison, Evaluierung des Cyber Lagebildkonzepts im praktischen Einsatz. Cyber Situational Awareness in Public-Private-Partnerships: Organisationsübergreifende Cyber-Sicherheitsvorfälle effektiv bewältigen (2018): 293-344.

regulations regarding the payment of ransom, the value or information in combination with risk transfer strategies like cyber insurances, potential damage unavailable and/or leaked data might cause to the organization itself or partners/customers, as well as legal implications with respect to regulatory requirements that are caused due to leaking said data, e.g. GDPR-related issues, SOX or others. While the decision, whether ransom is paid is typically conducted by NPCs in classical technical exercises and is seen as a way for the exercise management to end the scenario, or even railroad the players back on track after misjudging technical issues, these questions can be far from trivial in a real-life situation.

Handling new legislation: Recent developments in the area of regulations make legal expertise extremely important. Starting with the GDPR and the implied sanctions, as well as penalties, legal advice in cyber incident handling is also a financial issue. With the advent of the NIS 2 the requirements of the NIS are also becoming relevant for a lot of companies not typically localized as a critical infrastructure. The continuing development of new legislative documents like the DORA or the Digital Services Act / Digital Markets Acts with conflicting targets and definitions make the whole legal landscape surrounding cyber security increasingly complex. These existing and new legislations can cause severe complications in the case of a cyber incident. Furthermore, scenarios focusing on such new legislation might not even simulate a cyber incident at all, simply simulating a due diligence or audit process, or even the effects of actual jurisdictions or surprising decisions of a court results in important scenarios for simulation.

New data and technical processes: The introduction of a new technology or a new product, without the presence of an attacker, is another class of use-cases for such tabletop exercises, especially when the legal department was not informed about the capabilities of the new system at hand that and could not conduct an analysis with respect to technical regulations like e.g. the AI Act or the GDPR. Special stress can be generated, when this new software has already been put on the market, e.g. in the form of Software as a Service (SaaS) and legally grounded decisions need to be made whether to continue or to shut down the system. Additional modification of this use-case can incorporate the introduction of new and sensitive data streams into a system, that until now was uncritical, or the utilization of a previously uncritical system for high-risk operations. These challenges increasingly gain importance, especially in the light of new regulations focusing on data usage and its inherent risks.

Implications of technical cyber incident handling: New legal requirements are not the only challenge for legal experts in cyber security cases. Especially during incident handling, technicians are sometimes tempted to introduce technical and/or organizational mitigations that have legal issues. For example, they could exchange information with external experts or even competing companies that could pose a privacy or security issue. They might prioritize incidents and actions based on pure technical criteria, but not on legal requirements, like e.g. notification of customers or providing incident documentation to authorities. Another issue could be relying on untested solutions and their potential for damage, which might cause additional liabilities. Also, the utilization of grey market tools, e.g. special forensics tools, might raise legal issues, especially in state actors and with respect to proliferation, as many of these tools operate on the grey market, buying exploits and thus financing professional cybercrime, thus introducing a completely new angle of legal and even ethical questions.

3.2. New Technologies, Players and NPCs

With the increasing demand for AI driven technology, new problems arise requiring combined efforts in technical, as well as legal, dimensions. This not only focuses on the need to adhere to new regulations like the upcoming AI Act, but also to much more mundane, yet important issues that we will outline in this section. In order to illustrate the effects of new technology on legal cyber incident handling, we will use two technologies that garnered a lot of attention throughout recent years: Artificial Intelligence, especially Machine Learning, and public Blockchain solutions.

New regulations like the AI Act feature a lot of challenges for the introduction of AI into an organization, especially if the application field and/or the application itself is categorized as belonging to the high-risk category. In addition, the AI Act also sports definitions for prohibited applications, especially by governmental agencies. Organizations introducing high-risk AI need mandatory risk assessment, which is currently problematic for some classes for algorithms like neural networks. But even for lower risk classes, there might be issues of controllability and liability. These classes of algorithms face the so-called explainability problem, i.e. even with perfect information on every state of the network, all training and all processing data it is currently not possible to explain, why an algorithm reached a specific result. This has some serious implications during incidents, as identified errors typically do not lead to a general solution for the problem, like in the case of normal vulnerabilities. Handling this situation is a very delicate task from a legal perspective, requiring a lot of knowledge on the possible dangers resulting from the specific system behaving potentially erroneous in certain instances. Even further, it might become questionable, what the neural network is actually trained to detect.

Another important topic for legal cyber exercise is the topic of algorithmic bias, i.e. the propagation of prejudices that are somehow manifested in the training data. This also opens the question on who trained the data, which is much more important in the case of neural networks when compared to standard software, as the data has a huge impact on the trained model and thereby on the system (data defined software). Since training will often be done externally by specialized companies, these new entities require simulation (NPCs), which can be very complicated as they hold very special knowledge that is not simple to simulate.

Public Blockchains on the other hand face the very typical problem of data removal. Since blocks committed to the blockchains are typically immutable, the maximum that is possible is tracing back to the problematic data block and either forking the blockchain while trying to get rid of the block, or trying to remove the problematic block and then re-doing all subsequent blocks in their respective order. Both strategies are extremely costly and often virtually impossible to achieve, especially the later requiring a lot of control over the blockchain and the buy-in of a large majority of coin holders, if it is possible at all. While this is typically seen as a feature of blockchains, this can be very problematic in case of illegal information having been pushed onto e.g. a blockchain based data store. Furthermore, it involves the coordination of largely unknown other entities with their respective agendas (NPCs), something which is extremely complicated even in small blockchain installments and next to impossible in large ones.

As can be seen based on this short outline, new technologies introduce a lot of new training scenarios for a legal perspective, as well as complicated NPCs that might be very hard to simulate.

3.3. Exercise artificialities and challenges for legal scenarios

Exercise artificialities describe artifacts introduced into the scenario and the exercise execution based on the nature of the simulation itself[13], i.e. the effects of playing an artificially simulated game instead of being in the midst of an actual cyber incident. These artificialities impose a lot of additional challenges, some typical for these kinds of exercises but noteworthy for the legal part, other novel for exercises focused on the legal aspects of cyber incident handling when compared to classical cyber tabletop exercises focused on technical issues. In order to generate the best training effect from an exercise, it is of the utmost importance to consider the effects of exercise artificialities and their impact on (i) the scenario and exercise itself and (ii) the training results. Following, we identified the most important artificialities when designing and organizing exercises focused on legal issues in the cyber domain.

[13] Kaundert/Ziegler/Pahi/Skopik/Leitner/Kieseberg/Schwanzer/Ampia-Addison, Evaluierung des Cyber Lagebildkonzepts im praktischen Einsatz. Cyber Situational Awareness in Public-Private-Partnerships: Organisationsübergreifende Cyber-Sicherheitsvorfälle effektiv bewältigen (2018): 293-344.

Scenario complexity: On one hand, the scenario needs to be complicated enough to cover vital topics and current, relevant risks, and it also needs to be complex enough to be interesting for the players in order to generate the motivation that is necessary to imitate a real-life stress situation. On the other hand, given the time constraints and simulation restrictions imminent in exercises, scenarios that are excessively complicated might not even executable or will most likely result in feelings of frustration and exposure to hazardous amounts of stress. Therefore, striking a balance between the complexity of the scenario is a very difficult work that involves not only a strong understanding of technical and legal topics related to information technology, but also an in-depth examination of the organization, as well as the skill levels of the participating players.

National characteristics: While purely technical exercises can be played in international teams and are largely immune to location changes, this does not hold true for legal aspects of cyber incidents. While many regulations are quite similar in e.g. the European Union at first glance, even regulations like the GDPR have their national counterparts that need to be taken into account and have their own individual peculiarities. Furthermore, many legal aspects are still regulated on a national level, even inside the EU and need to be analysed in context to higher-value legal interests. The complexity even increases when conducting an exercise scenario involving international partners, or even just international subsidies of the same company. This additional complexity needs to be considered, as it is a major differentiator to technical cyber tabletop exercises. Of course, these issues can be the exact reason for actually conducting the exercise in the first place, and it provides a very good scenario in many cases related to cyber incident handling due to having to manoeuvre in this international legal sphere, still, it requires even more preparation effort on the side of the exercise management.

Timing: A cyber exercise is a very condensed and time-limited endeavour. While a real incident might play out over the course of several days, this is not possible to simulate in most environments due to legal, practical and budget reasons. There are exceptions of course, like the exercises organized by ENISA, but even then, a fixed timeframe needs to be provided for the exercise, which is not possible in real life incidents. Furthermore, attackers do no tend to honour classical working hours in real life, rather attacking in the evening, on weekends or even holidays. In addition, the condensed nature of a cyber exercise typically does not leave enough time for a real, in-depth legal analysis, so the players will (i) either have to give short opinions without the rigor typically inherent to legal advice, or (ii) resort to pre-analysed results that are then applied in the context of the exercise scenario.

The required players: One of the most essential parts is training the appropriate participants. Although this may appear to be a self-evident statement at first glance, particularly in the context of exercises designed for management, it actually necessitates the participation of staff who are located at extremely high levels within the hierarchies of the relevant business. While this is already a problem in technical scenarios, it is often possible to simulate these levels, as the focus does not lie on the legal ramifications of decisions, but rather on their technical and operational execution. This is completely different when exercising the legal aspects of cyber incident handling, where these very ramifications are an essential part of the simulation as a whole. In many cases, it is quite challenging to align these requirements with schedules, particularly in scenarios that involve multiple organizations. In addition, even if all of the necessary individuals have been approved, there is still the possibility that significant day-to-day business will interfere. Thus, the exercise management will need to be able to react to such problems with very fine-tuned simulations, which not only requires a lot of foresight with respect to the solutions and legal issues the legal experts in the simulation will come up with, but also a lot of additional preparation efforts in order to be able to simulate the decision-making process.

Maintaining stress: The development of an appropriate and realistic degree of stress is one of the most significant challenges that arises throughout an exercise. This is especially true given that everyone is aware that the stakes are not genuine. This is especially true for legal analysis, which most likely cannot be conducted the proper way in the exercise due to time constraints, which might result in staff not experiencing the stress level planned for the exercise and realistic in real-life situations. This could be circumvented by preparing the analysis beforehand and only requiring quick decisions by the players, or by acting in known terrain, e.g. in a scenario, where the guidelines for dealing with the eventualities have already been devised and only need to be applied. For example, a company could already have rules in place for dealing with blackmail, as well as handling loss of private information and the exercise scenario could focus on an ransomware combined with extortion, i.e. the attackers not only encrypted the information, but also stole it and threaten to publish it in case no additional ransom is paid.

Simulating technical aspects: While in standard technical scenarios, the players know the infrastructure that is simulated to be under attack, this does not necessarily hold true for a legal cyber tabletop exercise. This not only cover in-depth technical expertise, but also rather mundane information, e.g. the backup strategy of a company and the protection of said backups e.g. in case of a ransomware attack. This technical expertise needs to be taken care of in order to enable the players to arrive at the correct legal conclusions, e.g. regarding requirements for customer information or in order to correctly assess the severity of an attack when deciding whether a notification of governmental agencies in required, or not. While this expertise can of course be simulated by the exercise management, it is very beneficial to introduce some technical experts of the systems in question as simulators to the exercise.

Information overload: The timeframe is quite rigorous in these kinds of exercises, and it is impossible to process a large amount of information in a short amount of time. As a result, these kinds of exercises may lead to the realization that less information is more important. As has previously been seen in actual exercises, the high time constraint renders additional knowledge meaningless, even though it would be extremely important in case of real-life legal analysis. This might be conflicting with real-life scenarios where, given that actual situations often take place over a much longer period of time, this knowledge does not act as an additional obstacle at all. In other words, the fact that the exercise is so condensed could lead to erroneous conclusions regarding the usefulness of information that is readily available. This is especially important in cases where the simulation is not used to test the players, but as a means for determining which information needs to be collected and stored in a system.

Happy Ending: Especially when it comes to conducting exercise scenarios that include the management level, failure is not an option. This means that the exercise can end with comments for development, but an overall negative experience is avoided, even in situations where there is a clear failure. This is especially important for legal scenarios that include highest-level decision-making based on legal analysis conducted during the exercise. A number of factors, including but not limited to the following, may be negatively impacted as a result of this: (i) the complexity of the scenario that is necessary for a steep learning curve; (ii) the formulation and kind of feedback that is provided; and (iii) the originality of the simulated attacks. There is a possibility that this problem might be rebalanced through the implementation of extra internal feedback loops, without the participation of external individuals or management at a higher level in the hierarchy. Still, especially when conducting these exercises in order to get better knowledge on the actual reaction of an organization to certain incidents, the result of the exercise might not be positive. Contrary to pure technical scenarios, railroading the players to reach the correct solution might be very difficult or even next to impossible.

4. Conclusion & Future Work

Cyber tabletop exercises have emerged as an important tool for training staff on how to deal with cyber incidents. While these exercises currently mainly focus on pure technical issues, with legal questions typically only considered as side-issues, in this work we showed that tabletop exercises can be an excellent tool for training legal personal in dealing with legal implications of cyber incidents and the side effects of technical cyber incident handling. Furthermore, it can also be an excellent tool for training legal experts on how to deal with new jurisdiction in this area. We conclude that providing cyber tabletop exercises specifically tailored for legal experts in information technology can be a valuable asset for making organizations more resilient against malicious intent. In addition, the organization of such exercises can draw on the large body of knowledge and experience in conducting technical cyber tabletop exercises, thus allowing for the efficient re-use of many scenarios, planning tools like cyber security canvas and personas, as well as the integration of legal aspects with technical trainings.

In the future we plan to conduct a series of tabletop exercises focusing on the legal aspects of cyber incident handling together with legal experts in order to detect hidden differences and challenges, as well as defining useful Key Performance Indicators for successful cyber trainings in the legal field.

5. Literatur

Ecso. Understanding cyber ranges: from hype to reality (s. 31) [wg5 paper]. Https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf : s.n., 2020.

EUROPEAN COMISSION, Proposal for Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, COM/2021/206 final.

EUROPEAN COMISSION, Proposal for a regulation of the European Parliament on digital operational resilience for the financial sector and amending Regulations. (DORA)

EUROPEAN COMISSION, Regulation (eu) 2016/679 of the European Parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 (2016)

Gafic Melisa/Tjoa Simon/Kieseberg Peter/Hellwig Otto/Quirchmayr Gerald, Cyber Exercises in Computer Science Education. In ICISSP (pp. 404-411), 2022.

Kaundert Miriam/Ziegler Louis/Pahi Timea/Skopik Florian/Leitner Maria/Kieseberg Peter/Schwanzer Bernhard/Ampia-Addison John Kojo, evaluierung des Cyber lagebildkonzepts im praktischen einsatz. Cyber situational awareness in public-private-partnerships: organisationsübergreifende cyber-sicherheitsvorfälle effektiv bewältigen (2018): 293-344.

Kucek Stela/Leitner Maria. An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. Journal of Network and Computer Applications, 151. 2020

Nagarajan, Ajay/Allbeck Jan/Sood Arun/Janssen Terry, Exploring game design for cybersecurity training. In 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 256-262

Ottis Rain, Light weight tabletop exercise for cybersecurity education. Journal of Homeland Security and Emergency Management, 11(4), pp.579-592, 2014