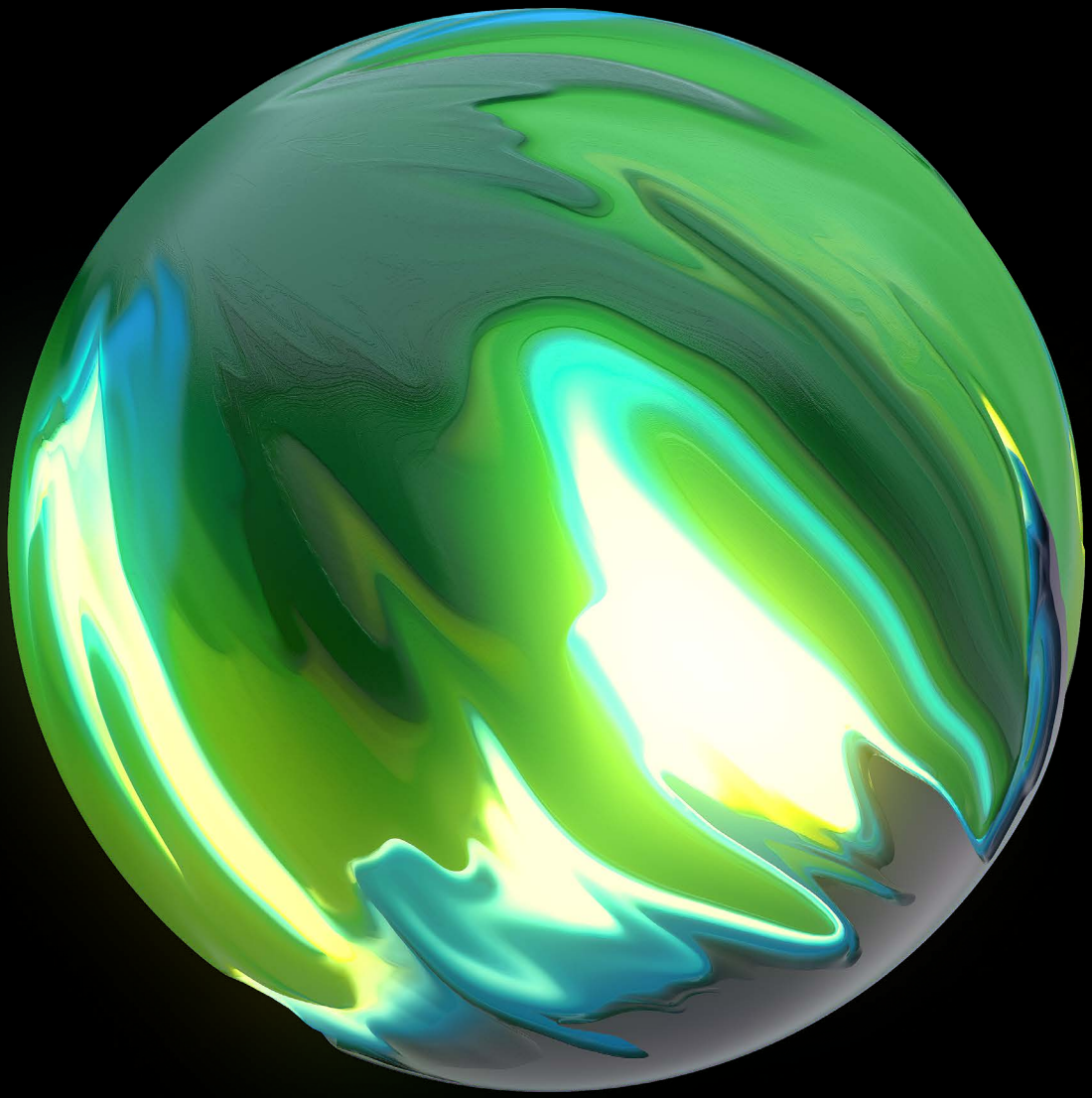
Deloitte.



Cybersecurity

The supreme discipline for agile organizations and cybernetic governance

MAKING AN IMPACT THAT MATTERS since 1845


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
if _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modifier object
rror_ob.select= 1
difier_ob.select=1
y.context.scene.objects.active = modifier_ob
int("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0

Preface

Advancing digitization, global use of cloud technology, Web3 or 5G telecommunications: all these technologies are opening up ever more comprehensive and diverse opportunities for people, companies and societies to cooperate, interact and communicate.

At the same time, they represent a completely new dimension of complexity of potential risks for cybersecurity experts in companies. Technological aspects and the relevant IT knowledge needed to cope with this complexity are intensively discussed in numerous publications and professional congresses.

This compilation of articles focuses on those aspects of cybersecurity that are often overlooked in the current discourse. The authors address the question of how companies should deal with cyberrisks organizationally, managerially and individually.

How do CISOs structure teams with their experts? How should communication and cooperation be structured to ensure the smoothest possible interaction between all those involved and affected in combating and preventing cyberattacks? What do managers need to pay attention to? What approach favors bringing CISO team experts into productive dialog and constructive cooperation on cyber defense with the entire organization? What does addressing cybersecurity mean from an individual perspective?

From a conversation between Dr. Ralf Schneider and Andreas Slogar for an episode of the Deloitte podcast "Sprint! New Work – New Mindset", the idea emerged to shed light on these perspectives on cybersecurity and to delve deeper into them with a number of well-known experts. At the heart of these reflections is cybernetics: the science, art or craft of control – and more generalized control, regulation and guidance – through communication, as defined by Prof. Dr. Fredmund Malik in his contribution.

This science encompasses a multitude of models, tools and insights that are becoming more and more prevalent in companies – i.e., highly complex systems – and whose potentials make it possible to use and manage the opportunities and risks of the technological developments mentioned at the beginning, instead of failing due to excessive demands. From this perspective, the co-authors consider the role of management in organizations in their contributions. They examine the structures of cooperation in companies and the effects on the individual perspective of employees in the context of cybersecurity and cybernetics.

Dr. Karsten Nohl kicks off the following reflections with an insight into the current situation of cybersecurity. He describes the dynamics of the race between hackers attacking companies and the cybersecurity teams fending them off and protecting companies from cyber risks.

Based on this, the transcript of the aforementioned podcast conversation can be found. Ralf Schneider describes from Allianz SE's global IT practice how their experts, CIOs, CISOs and he proceeded to think and execute cybersecurity in a completely new, participative and decentralized way using the power of cybernetics.

In his contribution, Prof. Dr. Fredmund Malik provides a focused insight into cybernetics, the development of this interdisciplinary science and its importance, especially in our century of networking.
In the fourth chapter, Andreas Slogar examines the organizational and collaborative structure perspective of CISO teams and discusses those elements of cybernetics that enable cybersecurity professionals and the organizational units of a company that collaborate with them to constructively and proactively address real-time events.

Finally, Yip Thy-Diep Ta focuses on the individual aspects of the subject area and the elemental role of antifragility and mindfulness in the context of cybernetics for each employee. Additionally, she develops a shift in perspective from the current need for action to future developments expected from the evolution of Web3 and the token economy.

As the publishers, we at the auditing and management consulting firm Deloitte would like to especially thank the authors and hope that you, our readers, will gain useful impulses for yourself and your colleagues from the following reflections, experiences and insights and thus be able to further develop your own work as a CIO, CISO or cybersecurity expert and rethink familiar paths thanks to new perspectives

Hacking protection – a never-ending competition inside of companies?

Dr. Karsten Nohl | Autobahn Security GmbH

Dr. Karsten Nohl is a hacking expert and founder of Autobahn Security in Berlin. Karsten creates awareness for cybersecurity – through hacking research and consulting. He is particularly fascinated by the trade-off between security and innovation.

The topic of hacking guarantees exciting Hollywood moments. In the real world, however, we are making little progress on hacking prevention. Both for the same reason: The actions of hackers seem to be mysterious because most people know little about them. For some, this mystery is a thrill; for others, it's the constant fear of becoming the next victim.

This fear often turns into lethargy for companies: "Hackers always win anyway". This attitude couldn't be further away from the truth: Companies record hacking attempts every day, and yet almost all companies are not hacked almost over all time.

To deal with cyber risks more confidently, we need to replace fiction with facts. We have already succeeded in reaching a fact-based perspective in other risk areas, such as the race against biological viruses. Although our understanding of biological organisms is rudimentary, we have successfully reduced the risk of many diseases through diagnostics, immunization, and treatment.

Technical systems and organizations are highly complex, but nowhere near as complex as biological organisms. Anyone who sees an opportunity to actively influence the risk of disease cannot throw in the towel when it comes to cyber defense. The first step of this journey: Through continuous measurement and decentralized improvement — that is, through cybernetics — we can demystify hacking and reach the necessary level of protection.

Hacking is steeped in myth because we talk a lot about hackers, but rarely with them. The most important step here is to understand hackers and their approach. Large companies do this regularly by inviting security experts to attack simulations. Those are similar to military maneuvers in peacetime: Some of your own troops play the enemy to find weaknesses in your defenses. The name given to the hacking maneuvers, red-teaming, also comes from the military — symbolically, the enemies wear red uniforms.

In the first step, the red-teamers gain control over a single company computer. This happens, for example, via email malware or vulnerably websites. In most cases, the initial gateway is not a critical system, but it allows the hackers to peak around the internal company network. In the second step, the red-teamers exploit vulnerabilities they find in internal applications and servers to incrementally expand their access over a period of weeks. In most cases, the hacking journey from the initial foothold to the complete control of corporate IT takes less than a month.

Red-teaming replaces nerve-tingling with facts on how hackers go about penetrating the organization's systems.
Each red-team exercise exposes the weakest link in the protection chain and what it takes to keep real hackers from breaking through. Red-teaming is not the only way for companies to understand hackers. The alternatives are retrospectives on real security incidents that provide similar insights, but only after the damage has already been done.

Based on the red-teaming insights, the organization can focus on making life harder for the next hacker. Regular red-teaming simulations – or real security incidents – enable improving the weakest protection links incrementally.

Continuous improvement raises the next question: When has the company reached a sufficient level of protection?
Until now, this question has often remained unanswered since companies do not quantify their hacking protection, i.e., they do not know how easy or difficult it is for a hacker to obtain important data. This must change to enable predictable risk management. What is not measured is hard to manage. Companies need a yardstick

benchmark to learn from each other and keep up with hackers.

Quantifying security can escalate into a hyperactivity for many – often measuring dozens of technical metrics and comparing them over time. Like the weather report, the numbers go up and down without the organization knowing how to influence them. Measurements that do not clearly point to opportunities for improvement are thus not useful.

Instead, a sensible metric is: a) accessible, even to security laypeople, b) formulated from the hacker point of view, and c) actionable, i.e., pointing to improvement steps.

Here the Hackability Score as a normalized benchmark that provides these three qualities is very useful. It aggregates a large number of security measurements from regular security scans. This raw data is already available at most organizations. Security scans of large companies regularly find several 100,000 vulnerabilities, but most of them do not help a hacker or a red-teamer. As a result, the scans cause more confusion and condemn security teams to frustrating extra work.

When summarizing the raw scan data into the Hackability Score, one question is asked for each measurement point: How much does it bother a hacker if this vulnerability disappears? Thereby, it is clearly specified which suggested actions are prioritized: Those actions that lower hackability the most also make life the hardest for hackers. This is confirmed by the next red-team exercise, at the latest.

Since the Hackability Score is always calculated in the same way – for each organization, each team, or each network segment – it enables a dialog between peers, for example between national subsidiaries of a group. The score illustrates who can learn the most from whom on which topic. And it is just one example of a standardized metric that enables dialog about cyber risks – even between experts and laypeople. Every company needs such a yardstick and needs the dialog between peers.

An easily accessible metric automatically turns into a race: Who can improve its Hackability Score the fastest and in the most sustainable way?
The challenge is decentralized: Every company, every domain, every team compares itselve to its peer group. Since no one wants to have below-average protection, and most even strive for well above-average hacking resilience, the race goes on and on – a positive cycle of continuous improvement. This way, the company achieves the desired demystification of hacking and makes progress on hacking protection transparent, which further fuels the improvement race.

One last ingredient is necessary to allow the virtuous cycle to run undisturbed: the organization's confidence to drive decentralized improvements. Instead of managing hacking protection centrally – as is still the case in many companies – the only task of the "risk managers" should be to provide decentralized teams with a target corridor for their Hackability Score. How a team achieves these goals is decided decentrally, often through shared learning in the peer group.

Hacking protection is achieved by:
1. Trust in decentralized self-organization
2. Friendly competition among peers (e.g., to reach a better Hackability Score)
3. Competition with real hackers (red-teaming)

Decentralized improvement based on a common measurement method, in a word, cybernetics.

Cybersecurity and cybernetics

A conversation between Dr. Ralf Schneider | Allianz SE and Andreas Slogar | Deloitte

The following interview with Dr. Ralf Schneider is based on a conversation that was published as an episode of the podcast "Sprint! New Work – New Mindset". This version is an edited transcription.

Dr. Ralf Schneider has been Group CIO of Allianz SE since 2010 and is responsible for IT Governance, Strategy and Security globally. Prior to that, he was Board Member for IT of Allianz Managed Operations & Services SE (2010–2016) and CIO of Allianz Germany (2006–2010). After his studies in mathematics and a PhD in computer science, he started at Allianz in 1995. For more than 25 years, he has held leading positions in IT, including department head of Information Systems Sales and department head of e-Business and Project Controlling Germany. In addition, he is a mandate holder of several cyber security organizations such as Cyber Security Sharing & Analytics e.V., the German Cyber Security Organization and the Digital Society Institute at ESMT.

Andreas Slogar has worked in more than 20 countries, the USA, Europe, the Middle East and Africa and has built up extensive experience in strategic and operational management work, including as CIO. As an expert, Slogar specializes in transforming entire companies into an adaptable collaboration state and is the author of various articles, podcasts and the book "The agile organization" (Hanser Publisher, 2018, 2020 – German).

Andreas Slogar: Ralf, you and your team have completely rethought and established Allianz Insurance's global cybersecurity based on cybernetics models. To start with, could you describe the problems you encountered in the area of cybersecurity? And how does cybernetics come into play?

Dr. Ralf Schneider: Allianz is a global company with many brands and operating units. And each unit has two key players in cybersecurity, the Chief Information Officer, who can change the systems and make them more secure, and the Chief Information Security Officer. In our case, that is 65 CIOs and 65 CISOs! Now the big challenge is: How do you get these 130 people aligned in implementing cybersecurity without everyone running in a different direction? When systems are this complex, there is only one answer: cybernetics, which is the science of self-organization, self-regulation and self-control. Because the main question of cybernetics is: How do you make the system control itself?

Andreas Slogar: In other words, it was not so much a technical problem that you had to solve, but an organizational one? How can you become more efficient, faster and more effective through self-organization?

Dr. Ralf Schneider: We move in systems that I like to describe as socio-cyber-physical systems. People are networked with other people or machines via software. And this networking is also feedback-connected. When you look at such systems, it's not only important what their process structure or organizational structure looks like. But also: How does the control structure actually work?

Andreas Slogar: Now cybersecurity is an increasingly relevant topic for all organizations, from companies to governments. What have you been able to achieve with cybernetics that traditional approaches don't allow?

Dr. Ralf Schneider: The starting point is the question: Where do you want to go in the first place? One of the most important cybernetic principles is: You need a common language that every acting person in the system understands equally. So we first formulated a policy that describes how cybersecurity is practiced in Allianz. This also defines the security controls and their implementation. Cybernetics now comes into play during implementation. We have implemented these controls in each of our 65 country organizations and then verified them through effectiveness testing. Cybernetics provides a model for the controls. The model makes it transparent what is going on locally in terms of cybersecurity, what risks have been identified, what dangers are lurking or what attacks are currently taking place. We have defined ten cybersecurity health indicators that are monitored centrally via sensors. This transparent control of the systems and feedback means that everyone knows what needs to be done.

> You have to give two things and ask for two things. What you have to give, of course, is trust. Trust that people will do the right thing, but also that they can do the right thing. That is very important, to hand over trust to your colleagues. And the second thing is autonomy. Giving them the means and letting them operate autonomously. Very important: Autonomy does not mean autarky.
>
> **Dr. Ralf Schneider, Allianz SE**

Cybernetics
Cybernetics is the science of controlling complex systems. It is based on the self-regulation of natural organisms and transfers these principles to machines or also to social systems. A well-known example of cybernetic control is a thermostat equipped with measuring and control elements. When certain thresholds of the actual value are exceeded, the heating system is counteracted in order to achieve the setpoint value. The term cybernetics goes back to the Greek word kybernetes ("helmsman"). In the course of its history, it was transferred from control engineering to the disciplines of information technology, philosophy, sociology, pedagogy and management theory, among others.

Andreas Slogar: Does every CIO then see these controls in a kind of dashboard? Or do you have working groups in which you look at them regularly? How do I have to imagine this operationally?

Dr. Ralf Schneider: That's exactly the right question, which brings us to self-direction. In cybersecurity, where an attack happens at the speed of light, you can no longer operate with committees. We use our so-called Cybersecurity Cockpit as a dashboard here, where all the information from the sensors is made available to us – centrally and decentrally – in real time. For me, the most central methodology of cybernetics is that everyone knows that you know. That means just that every single CIO is aware of what situation he is in, but at the same time he also knows where all his other colleagues are. And he also is aware of that all colleagues know that everyone has the same knowledge as he himself has. And that's in real time. That is the key. But the salient point now is: If the model of control is not sufficiently effective to ward off attacks, then you have to adapt the model until the necessary effectiveness is (again) achieved.

Andreas Slogar: And you adapt the model via the feedback of events. If there is an attack somewhere and this becomes visible in the dashboard, can you use this to iteratively develop the model further?

Dr. Ralf Schneider: Exactly. It is a dynamic model in two respects. First, the cybersecurity health indicators are adjusted according to the attack vectors. Second, new indicators are also created. In an agile organization, modeling is not supposed to represent the real world one-to-one. But the model must of course be effective. The beauty of cybersecurity is that you can tell very quickly whether the model is effective. If you find an attacker, you can fend him off or identify him, so you can always sharpen the model. And the punch line is that because the language is the same for all national companies through the policy, adjustments are equally and simultaneously effective for all of them.

Attack vectors
In cybersecurity, the term attack vector is used to describe the particular path or method that an attacker (hacker) uses to penetrate a system and cause damage. The term originates from biology or epidemiology, where vector refers to the carrier of a pathogen. For example, the anopheles mosquito transports the parasitic protozoa that then causes malaria in humans. In the IT domain, attack vectors typically exploit certain known weaknesses in the target systems ("exploits"). Vectors include buffer overflow, JavaScript vulnerabilities, network protocol vulnerabilities, or phishing.

Andreas Slogar: In a way, the transparency of the model forces everyone to cooperate. Is this how it is used – or is everyone now competing to see who can be quickest in combating attacks?

Dr. Ralf Schneider: I'd like to turn it around. It doesn't force cooperation, but it gives the group the ability to do so. You should see the possibilities, not the coercion. That's a huge advantage in cybersecurity. After all, you have a common adversary. The attack is not limited to one national company; you are always a community of fate. Cooperation and best practice sharing always win out. You don't try to develop the best defense method yourself; instead, you cooperate and follow a common standard. In addition, the decentralized use of cyber defense tools is practiced in training sessions, not the invention of new defenses. This, in turn, takes place centrally.

Andreas Slogar: You mentioned the topic of "agile organization". The immediate reaction to a dynamic change in my environment is exactly what was promised by the agile movement, whereas you are in the supreme league of dynamics here, where changes occur at "the speed of light". I can't discuss a cyber threat first; I have to have my actions on the table and apply them immediately in a self-organized way. Can this cybernetic principle be applied in other areas of an organization?

Dr. Ralf Schneider: Absolutely. I'll take a little trip back in time. It was 2008 or 2009 when I first got in touch with the agile manifesto, we implemented that as well. In an agile organization, we always applied the following important principle: You have to give two things and ask for two things. What you have to give, of course, is trust. Trust that people will do the right thing, but also that they can do the right thing. That's very important, to hand over trust to your colleagues. And the second thing is autonomy: giving them the means and letting them operate autonomously. Very important: autonomy does not mean autarky. For an effective and efficient agile organization, taking responsibility is critical. Responsibility then stays where you put the trust. That's central. I can't trust at the same time and then not know what's happening. Transparency represents a very important cybernetic principle. Not nit-picking, but as transparency about the effectiveness of the autonomous units, kind of like on the soccer field. As a coach, I see how effective my autonomous units are and I can intervene by giving instructions, changing the strategy, or even substituting someone. In cybersecurity, there is no getting around the autonomy of the agile organization. In management in general, in IT management in particular, and in cybersecurity in specific, we have a blind spot so far. But you can no longer manage in a Tayloristic way or with the division of labor. The only way is through self-organization. The person who fends off hackers "on the front lines" must act autonomously. However, he or she is in touch with the central system and makes it transparent what he or she is doing at any given time.

Agile organization
Agile organizations are characterized by their ability to learn and adapt quickly. In contrast to hierarchical organizations, they feature open structures and compressed decision cycles. Teams are maximally autonomous. Prerequisites include transparency and effective feedback loops. Agile organizations are particularly suited to situations characterized by a high degree of external uncertainty. The concept has become known primarily in the field of software development over the past two decades. In 2001, its principles were formulated in the "Manifesto for Agile Software Development", with reference to methods such as SCRUM and Kanban.

Andreas Slogar: So you have agreed on a common understanding and approach model in your cybersecurity policy. This is precisely how you remain decentralized, compatible with each other and capable of connecting. Everyone is responsible for applying the policy in his domain in a self-organized manner. And the transparency allows you collectively to establish an Algedonic Loop in order to achieve a feedback from the experiences and thus to further develop your model.

Dr. Ralf Schneider: Yes. In December 2021, we had a cyber issue with Log4j that we learned very well from because it was new to everyone. It became known that there was a vulnerability in a Java library, and practically every source code had to be scanned to see if this library was used. In Allianz Germany, two or three employees wrote a scan to find the vulnerabilities. And we were able to make those operationally available to the whole world immediately. Everybody could enter his IP addresses and check via the algorithm whether this threat from the web was there or not. I think in just three hours, 7,500 Allianz IP addresses were scanned.

Algedonic Loop
This term was coined by the American psychologist Henry Rutgers Marshall (1852–1927) and taken up by the British cyberneticist Stafford Beer (1926–2002). It refers to the control of an organism or system by incentive feedbacks such as pain and pleasure (from Greek: algos = pain, hedone = pleasure). If behaviors are optimized only to this incentive mechanism but no longer to environmental stimuli, there is a risk of counterproductive behavior.

Andreas Slogar: That is a scaling effect that speaks for itself. – But now a question about you: How did you actually come to cybernetics?

Dr. Ralf Schneider: Cybernetics came to me in the form of the economist Fredmund Malik. The subject was complexity, the control of complex systems. I met Mr. Malik in 2017, and he introduced me to cybernetics and, above all, how to implement it in management. A crucial model for this is the Viable System Model by Stafford Beer. It answers the question: How do you manage an organization cybernetically?

Log4j
Log4j is a widely used IT framework for automatic logging. Among other things, it is maintained as part of the Apache Logging project. Today it is used in many programming languages and applications. In December 2021, a vulnerability in Log4j version 2 was disclosed, allowing attackers to remotely execute program code on the affected system.

Viable System Model
The term Viable System Model goes back to the cyberneticist Stafford Beer. Instead of profit maximization, the survival of the system is set as the primary goal. Centralized control is less suitable for this than decentralized self-control of all system elements. Under the socialist president Salvador Allende in Chile in the early 1970s, Stafford Beer and others attempted to implement a computer-based decision-making system for controlling the national economy (Cybersyn) as a more democratic alternative to the Soviet command economy.

Andreas Slogar: Exciting, we are both big fans of Stafford Beer, Heinz von Foerster, the Viable System Model and everything that was achieved with it in Chile in the 1970s, for example.

Dr. Ralf Schneider: Yes, you have to think about that: He had already understood what it was all about and implemented it in Chile. If he had been able to use cybersecurity sensors, that would have been a highlight for him. They are very important today: You must have automated sensors! You can't rely on reporting channels in cybersecurity, because otherwise you're simply too slow.

Andreas Slogar: Now cybernetics is not very common in the business world. When you talk about it, people often stare at you very astonished. Why is that?

Dr. Ralf Schneider: I think it's because of this blind spot that we don't even see, that managers don't experience in their training and professional practice. People train very well and in a very structured way to make the right decision analytically. Do we go left or right, or do we examine it more closely and think about a third way? But in cybersecurity, you can't decide anything as a manager. You have to rely on the system and the people to make the right decisions. You can only work on the process, control and organizational model you use. And on a meta-level, you can work on how well employees are trained to use this model. In doing so, you actually have to unlearn everything you learned before as a manager. This also applies to gut decisions made by managers. In cybersecurity, they are quite bad – unlike gut decisions made by experts! The manager, on the other hand, should instead work on the model at the meta-level. But the problem is: We are all childrens of Taylorism and the division of labor. However, these are both structuring concepts that do not fit into cybernetics.

Andreas Slogar: That would mean that managers would have to turn their self-perception around 180 degrees. That they are not the ones who manage others and give them instructions. Instead, they are the ones who ensure that management is practiced as a skill in an organization. Managers observe this ability and develop it further. They establish self-organization, just as you have established it in your organization.

Dr. Ralf Schneider: Absolutely right! It's no longer about power over people, but power with people. That means building systems so that you're really effective. The better you are, the less you have to do as a model designer, the less work you have. But managers are conditioned differently. They think that the more time they invest and the harder they work, the more important they are. But it is exactly the other way around! The better your system runs in a self-organized way, the more effective it is. You need to focus more as a manager on how you promote and challenge the experts.

Taylorism
The American inventor and engineer Frederick W. Taylor (1856–1915) developed a scientifically based system of work organization, for example for factories. Taylorism is based on the principles of division of labor: Production processes are divided into various sub-processes, which can be carried out more efficiently by workers individually than if each worker carries out all the process steps (example: assembly-line production). Taylor backed up his approach with scientific time measurements of real work processes to ensure efficiency. The term is also often used critically to describe a rigid work organization.

Andreas Slogar: Now if someone wants to get into this fascinating subject, what tips would you have?

Dr. Ralf Schneider: Well, first of all I commend the book "Kybernethik" by Heinz von Foerster. The word "ethics" is very important here. Because with cybernetics you can control everything, even a surveillance state and a dictatorship. That's why cybernetics also needs a strong ethical understanding, otherwise you end up in dystopias. Then you should learn something about the Viable System Model. First of all, something Stafford Beer, and then also a book of yours: "The Agile Organization". Because you get to the heart of how that can be applied extremely well. Because the great art is not only to understand intellec-

tually what cybernetics is. You also have to put it into practice. And then you have to let go. Of course, that's hard. Fredmund Malik says I get control over control, not more control over people. That's a whole different mindset!

Andreas Slogar: I am very pleased that my book is so well received by you. I also find Ross Ashby's reflections on the subject of the requisite variety of organizations exciting. These are really great moments in cybernetic theory. But to bring that into the daily business routine, that's quite a challenge. You've applied that right away to the "premier league" to cybersecurity. But you could also start with smaller topics that are less demanding. For example, you could attend a Fredmund Malik course and then try out the application in your own organization.

Dr. Ralf Schneider: And you can easily check it in practice. If someone says they control cybernetically, then I would ask: Yes, where is your dashboard? And secondly, I would ask: How up-to-date is your dashboard? Real-time? You can tell a lot from that.

Andreas Slogar: Without giving away any operational secrets now: How does the journey with cybernetics continue at Allianz?

Dr. Ralf Schneider: To address highly complex systems such as cybersecurity in Allianz, one naturally comes immediately to IT. Generally, the same principle applies here. How do you manage IT run, IT change and project development? There is a reference point to the agile organization. As soon as ten or 15 people come together, you have a highly complex system. Then you need cybernetic control. This also applies to management, not just IT or cybersecurity. In management, hierarchies should only be used where they really have their strength: to give freedom and to distribute resources. But the actual operational control then runs decentrally cybernetically. This is how it is with humans. If every action were controlled by the brain, without self-control and self-regulation with homeostasis in the body, we wouldn't get five seconds further. Systems and organizations must also be built this way.

Requisite variety
The concept of requisite variety was coined by the British scientist W. Ross Ashby (1903–1972). His "Law of Requisite Variety" (Ashby's Law) describes the minimum degree of complexity (action variety) required by one system to control another and at the same time to have sufficient leeway to cope with the challenges (disturbances) posed by the environment. The system complexity must at least correspond to that of the disturbances.

Homeostasis
The term, which originates from biology, refers to the internal state of equilibrium of a dynamic system that is achieved by self-regulation, for example by the adaptations in the human body to a disease or after external influences. Physiological examples are blood sugar or heat regulation.

Andreas Slogar: This is a beautiful picture. What cybernetics explains to us is nothing else than what each of us practices in everyday life. It's just that no one is really aware of it. Paradoxically, however, when we are in the system of corporate organization, these hierarchical models suddenly gain power over us. And we hand over what we are capable of, namely self-organization and initiative, at the checkroom.

Dr. Ralf Schneider: Exactly. In the company, we are hung up on three big things. We want to plan everything, preferably with quarterly planning. We want to anticipate everything that's going to happen. We want to control everything down to the decimal place. But we know that complex systems can neither be planned nor controlled, and certainly not predicted. But we try to do it anyway, even though humans intrinsically do it differently. For example, when we have run into the wall a third time, we realize that our model no longer works. First we don't know the wall, then we recognize it. A fourth time we do not run against it. In organizations, on the other hand, it can happen that after the third time we still plan exactly the same again, a fourth, fifth or sixth time. If it doesn't work anymore, then "more of the same" simply doesn't help. In that case, organizations also have to change their model.

Andreas Slogar: That is a nice transition to finish with. I would now like to ask: What would you recommend to colleagues who want to implement this – in view of your experience over the last four years?

Dr. Ralf Schneider: First of all, be extremely humble. No longer believe that you can still understand the systems or distinguish between what is right and wrong. To make the best possible decisions, transparency is elementary, as I said. As an IT professional, I would say look at the data, turn data into information, use sensors, build an abstract model of your reality. Just as humans do. We don't see everything, but only a spectrum of waves and colors. Focus your modeling on the purpose of your business and learn to apply it very quickly. And a second recommendation: Develop a common language about the problem. I often find this lacking in companies. Maybe this is also due to my history as a mathematician. If I have a common language, by policy, then I can consider what controls I pull in to make my system work. Are the controls complete? Are they effective or efficient enough? That's the function of feedback. You shouldn't just think that something has been done wrong, but reflect on yourself and question whether the problem has been understood at all.

Andreas Slogar: Ralf, thank you very much for this look behind the scenes, and also for your outlook on what else can be done with it – if one takes this approach ethically seriously in the sense of Heinz von Foerster and also acts accordingly.

What is cybernetics?

Prof. Dr. Fredmund Malik | Malik International AG

The word “cybernetics” comes from the Greek “kybernetes”, which means helmsman and is the Greek root for terms like governor and governance. Cybernetics is the science, art, and craft of controlling – and, generalized, governing, regulating, and directing – through communication.

Prof. Dr. Fredmund Malik is a recognized management expert and chairman of management and advisory boards in business corporations. He is a pioneer of management cybernetics and complexity management. He was a member of the board of directors of the Institute of Business Administration and, in parallel, of the St. Gallen Management Center since 1977. He is the author of more than 15 books. His book "Führen Leisten Leben" (Lead Perform Live) was voted among the 100 best business books of all time. In 2018, he received the Life Achievement Award, the highest honor in the German management education system.

The fact that there is also a science behind this art needs not be considered in everyday life. It only becomes interesting and important when problems arise for the solution of which everyday understanding alone is no longer sufficient.

How the acknowledged ingenious mathematician Norbert Wiener came to cybernetics, why he called his book “Cybernetics” in 1948, and who else was important in this field is a story of its own. It should be mentioned here that cybernetics is perhaps the most important science of the 20th century and is shaping 21st century even today. The full book title is “Cybernetics – Control and Communication in the Animal and the Machine”. During World War 2, Norbert Wiener worked on the mathematics of self-controlling rockets.

From the 20th to the 21st century

Atomic physics has been discussed publicly much more intensively than cybernetics. It is cybernetics that is transforming the 20th century into the 21st. Its full implications will shape our century. They will fundamentally change our lives. Without cybernetics, there would be no computers and robots, no electronics and no computer science. There would be no rapid advances in biological disciplines or genetic engineering. The developments associated with cybernetics create risks, but even greater opportunities. Those who want to avoid the former and take advantage of the latter should study cybernetics.

It was cybernetics and the closely related fields of systems science and information theory that made it possible to understand and explain the third basic quantity of nature – information – and finally to use it systematically.

Until then, science officially “knew” only two elementary quantities – matter and energy. These are the “objects” with which the supreme disciplines of the natural sciences – physics and chemistry – dealt in the course of the Enlightenment. And to these they tried to reduce the manifestations of the world. There is no doubt that this approach to research has brought us an enormous increase in knowledge and, at the same time, its application in the form of technology.

The century of networking

Some scientists were never quite satisfied with the basic philosophy of the natural sciences. Something was missing – and something crucial. If you know that an object consists of about 15 kg of coal, 4 kg of nitrogen, 1 kg of lime, ½ kg of phosphorus and sulfur, about 200 g of salt, 150 g of potash and chlorine, and about 15 other materials, plus quite a bit of water – what do you know? Basically nothing.

Influenced by conventional scientific thinking and educated on the basis of its logic, few will think of answering: It depends on how you organize these materials ... But that is exactly what matters.

The raw materials mentioned are what we get when we break a human being down into its material components. Nothing remarkable remains if we take away from a living being that which makes it a living being. What is important is not the materials. What is important is their organization, the pattern, the order they exhibit, or the

in-forming that puts the materials in order. Life is not matter and energy; but life is in-formed matter and energy.

This is what makes cybernetics important. One of its most significant insights is that matter and energy are of comparatively little importance to the character and capabilities of a system. What a system is made of is important, to be sure. What is essential, however, is the information that orders and organizes the basic elements. This is what makes the building elements a system.

Networking with the life sciences – but independently

In addition to the enormous developments in the technical fields and in computer science, impulses come from the life sciences. There, in turn, they come primarily from the neurosciences, the study of brains and central neural systems. It is the latter that directs, controls, and guides an organism. Brain research without cybernetics is no longer imaginable today.

Cybernetics receives important impulses from here, but it is not identical with brain research. It is an independent science. The basis of cybernetics is the discovery that there are natural laws which determine the control and functioning of all systems.

It does not matter whether the systems are natural or artificial, and it does not matter whether they are biological, physical, technical, social, or economic. This is what makes cybernetics a transboundary – transdisciplinary – science, which in turn is something other than interdisciplinary.

This is what prompted Norbert Wiener's important, often overlooked or misunderstood subtitle for his book: ... in the Animal and the Machine ..., by which he meant the divide between the natural and artificial worlds that has hindered understanding of complex systems since antiquity and allows us to make the greatest advances today.

Design and management of agile cybersecurity organizations

Andreas Slogar | Deloitte

The work of cybersecurity teams who want to defend companies against cyberattacks increasingly looks like an unequal race between the hare and the hedgehog. The tale is not about a sports competition, but rather about an existential conflict – here between companies' cybersecurity specialists and the attacking cyber hackers. They use high-tech means and there are no rules. At least not for hackers. And just like with the race of the hare and the hedgehog, the winner is not the one who makes the greatest effort and tries harder and harder. It is the more creative and agile one who manages to stay one step ahead of his opponent or outsmart him.

Technical finesse and expertise are used by cybersecurity and hacker teams alike. The real differences in this conflict are entirely non-technical. Hackers are highly flexible, agile and creative. They can cause great damage, especially with patient trial and error and relentless experimentation. The hacker only needs to succeed once in his attacks to get to his target, no matter what his motives are. The cybersecurity teams, on the other hand, are forced to win – always and against everyone.

If we compare the organizational structures of hackers with those of cybersecurity teams, further differences become apparent. Hackers are self-sufficient or autonomous. They work in a completely decentralized manner and take an agile approach, i.e., they adapt their maneuvers to the opportunities and possibilities that arise. Because of the decentralized approach, their way of working appears distinctly resilient and redundant, even though this is not a primary characteristic but an emergent effect. The learning speed of hackers is very high, as success and failure are the source of continuous feedback and learning loops. RACI matrices and QA-tested business processes, areas of responsibility and decision-making authority do not matter. Nor do management structures. It is always the most effective attack that leads the way.

If, on the other hand, we look at the organizational structures and cooperation models of cybersecurity teams (CSTs for short) in companies, the aforementioned terms seem to be highly relevant in traditional CISO organizations. Role models, responsibilities and decision-making paths are predefined, competences are specified, and business processes are defined and documented in an audit-proof manner. The degree of autonomous or even self-sufficient freedom of action for CSTs and their employees in the entire CISO organization is fixed and usually limited by role and the overarching chain of command.

This comparison raises the question of what the design of a CISO organization and the collaborative model used within must look like in order to bring the benefits of the hackers' approach to the employees in the CSTs.

Classic CISO organizations – three archetypes

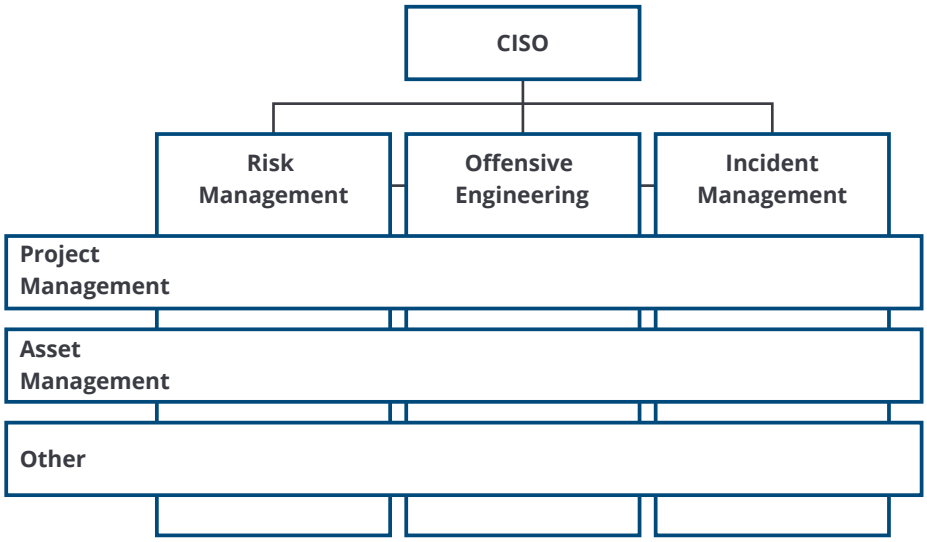
Let us look at typical organizational structures of CSTs and their organizational units, for which CISOs are predominantly responsible. After that, let us assess to which extent they can use or promote the characteristics of hackers' ways of working for their own approaches.

CISO organizations with flat hierarchies and matrix structures want to avoid redundancies in their business capabilities. They focus on ensuring the highest possible efficiency of the staff capacity deployed and the resources required. Such a focus tries to achieve an adequate level of performance and quality at the lowest cost possible.

This orientation works to the disadvantage of resilience and redundancy: Lost business capacity cannot be absorbed or at least temporarily taken over by an alternative function. Matrix organizations are also characterized by multiple communication and reporting channels. That leads to conflicts of objectives in the deployment and work planning of employees. Matrix organizations and organizational models with flat hierarchies try to find a compromise between the management's area of responsibility and the shortest possible communication channels.

Due to the multitude of communication channels between teams and employees, the primary goals of such an organizational structure are not achieved. Matrix organizations are therefore not suitable for maximizing the communication capacity of CSTs.

Fig. 1 – A.) Focus: flat hierarchy and matrix



Some CISO areas are oriented towards classic structuring forms of hierarchical organizational models. They let specialized departments and teams focus on specific subject areas or business capabilities, and show in which department or sub-department an individual issue or task is organizationally arranged. It remains unclear how this department and the respective employees cooperate with each other and with their environment.

The geographical focus of the organizational model is a variation of the previous structure. It is a scaled representation for globally operating companies that attempts to visually mimic established business capabilities. Thus, these organizational structures primarily adopt the representation forms of other business areas such as sales, marketing, or finance, but cannot represent the cooperation forms. Since national borders are irrelevant for cybersecurity events, this hierarchical organizational form is very limited in its information content and usefulness as an orientation aid.

The previous descriptions are deliberately pointed in order to more clearly delineate the alternatives described below. Certainly, no company has established one of these three archetypes in pure form. This distinction suggests solutions that each CST and CISO area can adapt and integrate in their processes to be able to act, to make fast decisions and enhance the efficiency of their own cybersecurity work to the respective requirements.

Fig. 2 – B.) Focus: business skills

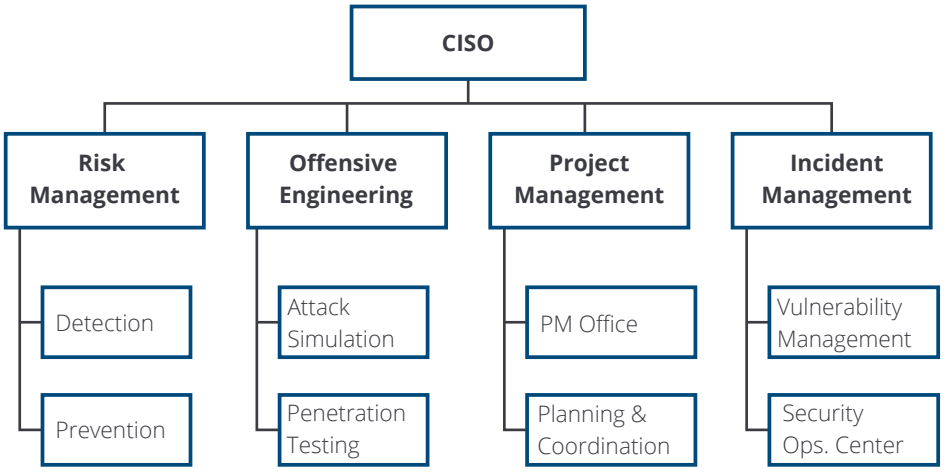
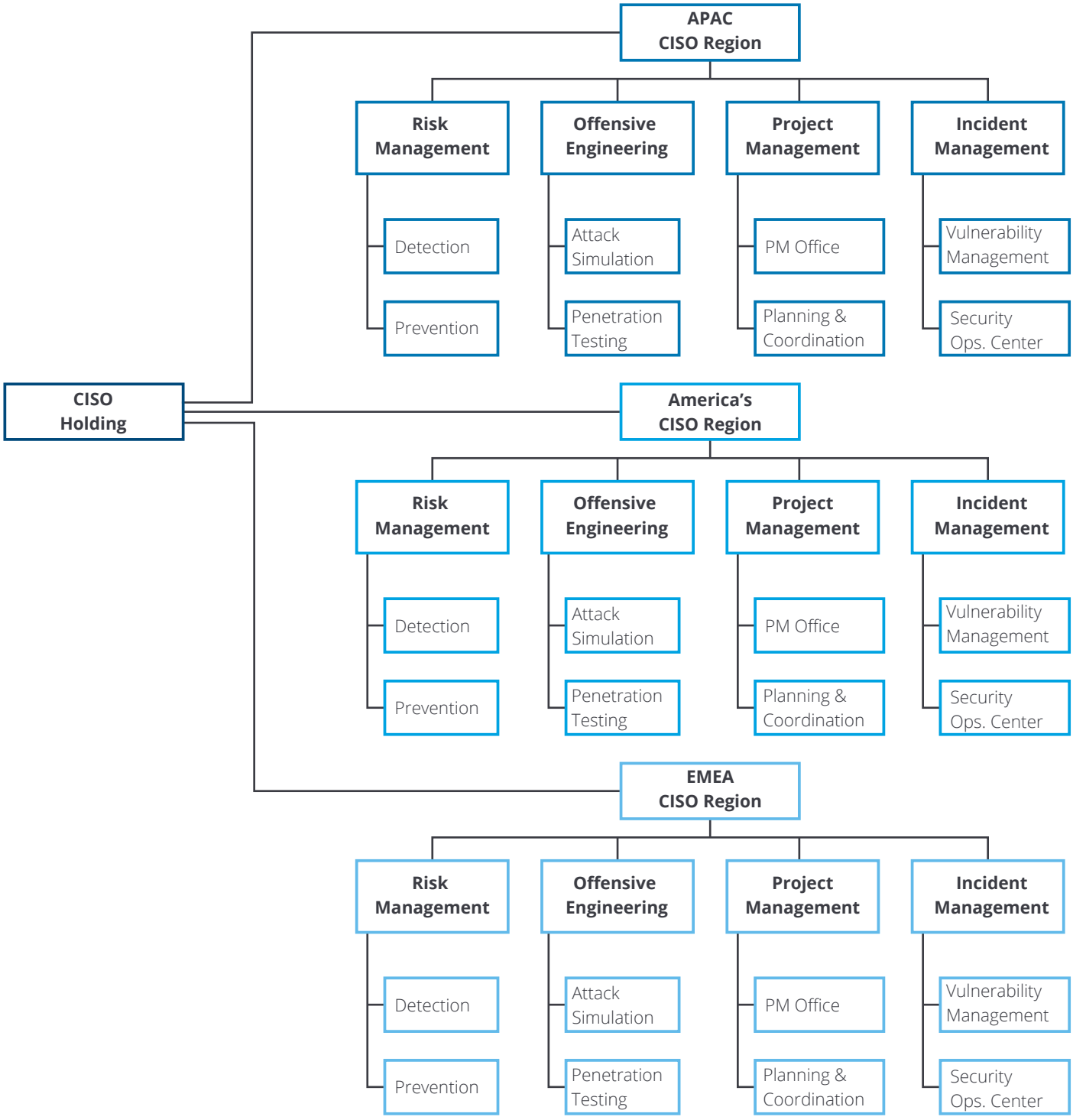
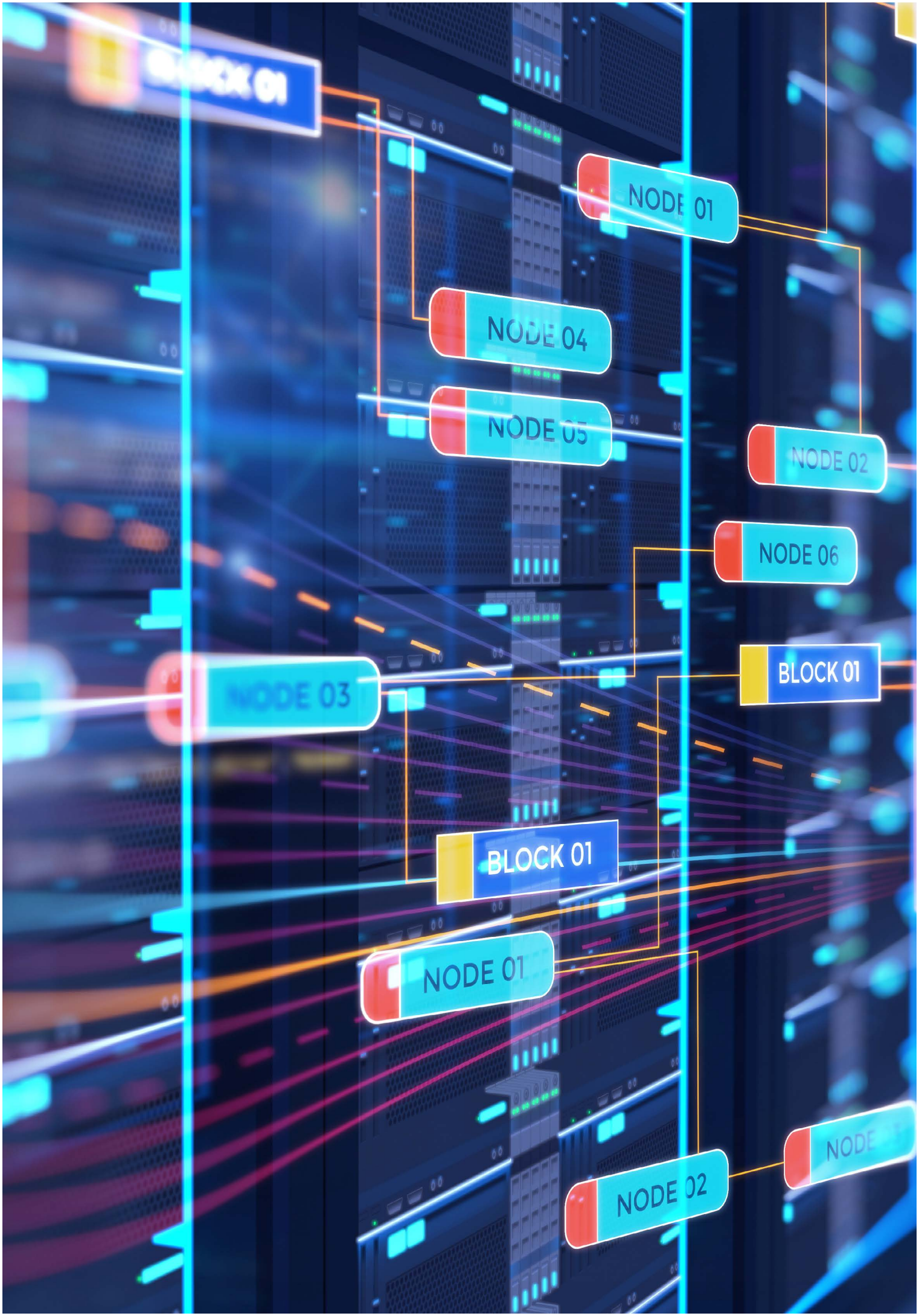


Fig. 3 – C.) Focus: geography




NODE 01
NODE 04
NODE 05
NODE 02
NODE 06
NODE 03
BLOCK 01
BLOCK 01
NODE 01
NODE 02

How much of a hedgehog is the CST?

In what ways do the listed archetypes of CISO areas and their CSTs support the characteristic features of the way hackers work in order to harness and benefit from them?

To find out, we have compiled these characteristic traits and compared them to the archetypes. Are they suitable for an integration into a CST's own work? Could they potentially support it?

Tab. 1 – Compilation of requisite capabilities

Property	Definition	A	B	C
Autonomy (decentralized)	Employees and their CSTs are free to act independently and self-organized according to their skills, competences, and knowledge.	No	No	No
Agility	Individual staff members and their colleagues in the CSTs are able to adapt the way of acting and cooperating, they have the required competences to change requirements, influences, and events.	Yes	Yes	Yes
Resilience	The available capacity of qualified staff and resources is sufficient to remain able to act and cope with an extreme stress situation over a longer period.	No	No	No
Redundancy	There is a "double bottom" of the CISO area to absorb existing skills and performance of staff and CSTs in case they fail in overload situations, attacks, illnesses etc.	No	No	Yes
Transparent and open communication	All staff members make all facts and findings available to each other without restriction; they interact openly and respectfully, they give each other appreciative feedback and thus ensure a psychologically safe cooperation environment.	Yes	Yes	Yes
Liquid Leadership	Depending on the use case or type of cyber security event, the most competent CST or the CST with the biggest knowledge on the topic of the event is in the lead role and provides the status of the triage, the identification of the attack vectors, orientation on the situation and the course of action to all the teams and experts involved.	No	No	No
Liquid Cooperation	Depending on the cybersecurity event, the required and most subject-specifically qualified CSTs and employees spontaneously come together in an adequate cooperation structure and organize themselves according to the Liquid Leadership Principle.	Yes	Yes	Yes
Feedback & Learning Loops	Facts and findings are consistently and regularly made available via established or institutionalized cooperation elements in order to be able to provide learning experiences via direct communication channels in the organization and to make them usable.	No	No	No

The elements of agility, transparent and open communication as well as the concept of liquid cooperation can also be operationalized in the archetypes listed. They can be observed in various companies. The ability to adapt to changing requirements and events in the context of cybersecurity and thus to proceed in an agile manner comes more naturally to CISO areas than to any other area of a company. The dynamic nature of cybersecurity events demands a minimum level of agility in addition to flexibility. CISO areas nevertheless tend to establish a procedure and cooperation structure that can be practiced in case of a cybersecurity event. It can be observed that these prepared structures are always dissolved in an emergency if the use case exceeds the possibilities. In such extreme situations, the employees automatically dissolve the existing structure, "liquify" it, so to say. A change to liquid cooperation can be observed. Therefore, it makes more sense to set up the cooperation structure according to the event in order not to lose time with adjustments and corrections in practical use.

As far as redundancy is concerned, only the geographically dispersed and self-similar CISO organization is potentially able to absorb the failure of business capability, a CST or individual experts, and continue to provide the required service. Organizations of the first two archetypes have, by design, little to no redundancy, which can be used in extreme cases. They are aiming at economic efficiency after all. Redundancies, even in CISO areas, are seen as cost factors to be avoided.

The situation is comparable to the characteristic of resilience. From an economic point of view and assessed as a disadvantage, it is mostly avoided. The lack of it usually leads to overload symptoms for employees in the CSTs and causes, for example, overtime, increased sick leave or even employee turnover. In contrast, a holistic analysis of these effects through a purely efficiency-oriented cost orientation is rarely carried out in companies in order to prioritize the relevance of resilience in the company.

Autonomy and liquid leadership are not or only rarely found in the archetypes described. Hierarchical organization designs are characterized by the fact that the decision-making authority and the responsibility for orientation in the event of an incident are located solely with managers. This concentration is economically understandable, but in the context of the high dynamics of cybersecurity events, it represents a critical limitation of the options for action and a reduction in the necessary speed of decision-making.

Feedback & learning loops are a growing topic in all companies, especially in CISO areas. They are understood as a value in itself. As far as sharing insights and building cybersecurity-related knowledge is concerned, these topics are predominantly focused on the specific responsibilities within the CISO area. Building cybersecurity insights and knowledge throughout the organization is mainly practiced as a communication one-way via training, online seminars, or communication measures such as email circulars and newsletters.

To promote company-wide knowledge about IT security and the awareness of employees that cyberattacks are critical events, interaction and communication between the CISO area and other parts of the company are necessary. Also, or especially in globally operating companies. Feedback is particularly relevant for the CISO in order to understand the level of maturity of the knowledge and behavior of all employees. In this way, a consistent information policy and training procedure can be planned and implemented for the employees.

Cybernetics for the design of a highly responsive cybersecurity organization

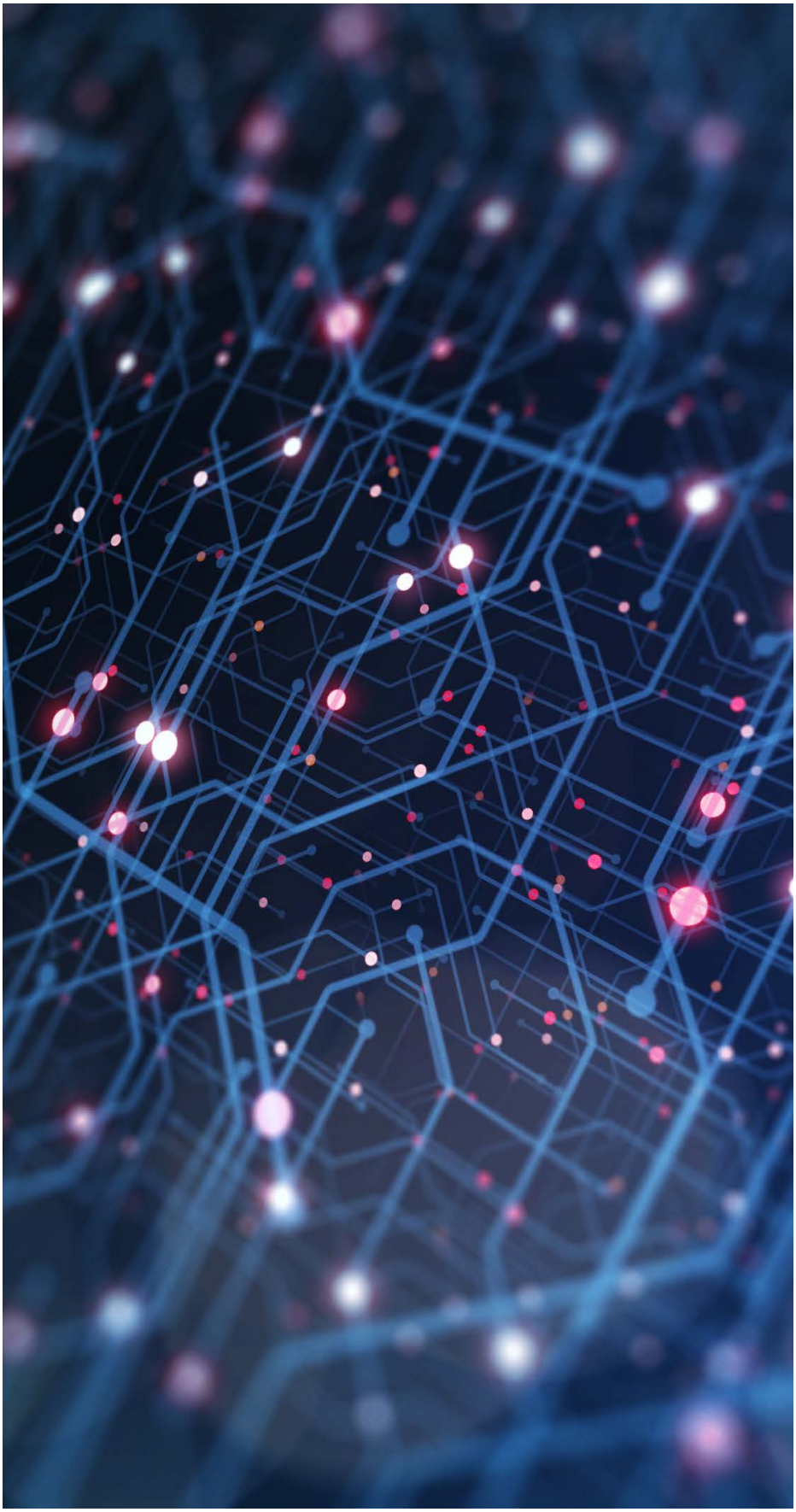
For the design of a CISO area with all its teams and business capabilities, we can make use of the findings of cybernetics on the functioning of complex systems. In doing so, we break away from the classic division of labor of hierarchical organizational models. As a model of thinking, it is very helpful to replace the concept of "responsibility" – for technical content or for decisions – with that of "contribution". In a complex system, it is always decisive what contribution an individual element makes to build up or ensure a specific characteristic or capability.

As an analogy the human organism can be used here. It consists of a multitude of parts that interact with each other via neuronal and hormonal communication pathways. Each of these organs, including the brain, makes a specific contribution to the development and livelihood of the complex overall human system. Questions such as who is in charge or who is "important" are completely irrelevant. In the interaction of business organizations, however, these questions are widespread and are dealt with at great expense.

One should move away from this to focus on the contribution of the individual elements and thus objectively adjust the design of the organizational model with its ability to act, adapt and thus exist. The latter is particularly relevant in the context of the CISO areas and the companies for which they are responsible.

To design a CISO area, it is appropriate to use an imperative by Heinz von Foerster and the Viable System Model (VSM) by British management cyberneticist Stafford Beer. Heinz von Foersters ethical imperative, which he based on the imperatives of Immanuel Kant, says: "Act always so as to increase the number of choices!"

This can be used as a basic design principle for CISO domains and all the CSTs grouped within. One has to ensure that every component of the organization, every team and every capability is planned and applied in such a way that the portfolio of options for action is continuously expanded when a cybersecurity event occurs or protection against one is needed. The focus on economic efficiency in CISO areas, as mentioned in the archetypes, reveals that these courses of action limit and do not expand the number of choices.



Stafford Beer developed his VSM in the mid-1970s and validated it in business practice. Thus, it is possible to design the functioning and interaction of an organization that can naturally process complex situations, i.e., unpredictable developments and events. In addition, the VSM enables to fully cover and ensure the previously listed characteristics such as autonomy, agility, redundancy, or transparent communication.

For the design of a VSM-based CISO area, the presentation to the listing of the own CSTs won't be limited but supplemented with essential elements. These allow to identify the basics for cooperation and the communication contents and channels within the own organization and the other divisions. So now the individual elements of a cybernetic organization and the integrated cooperation model for CISO teams will be shown in brief introductions.

Fig. 4 – Viable System Model

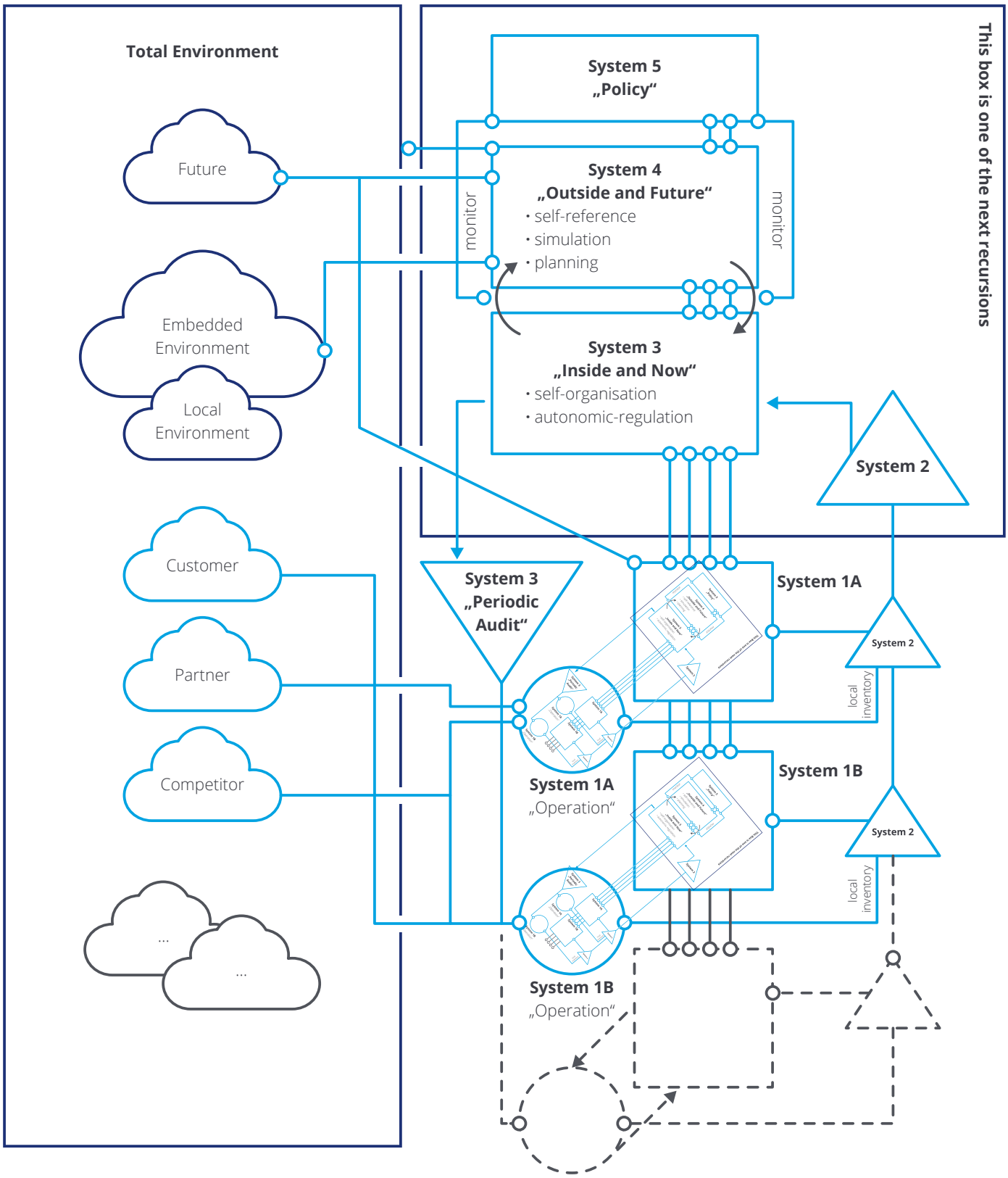
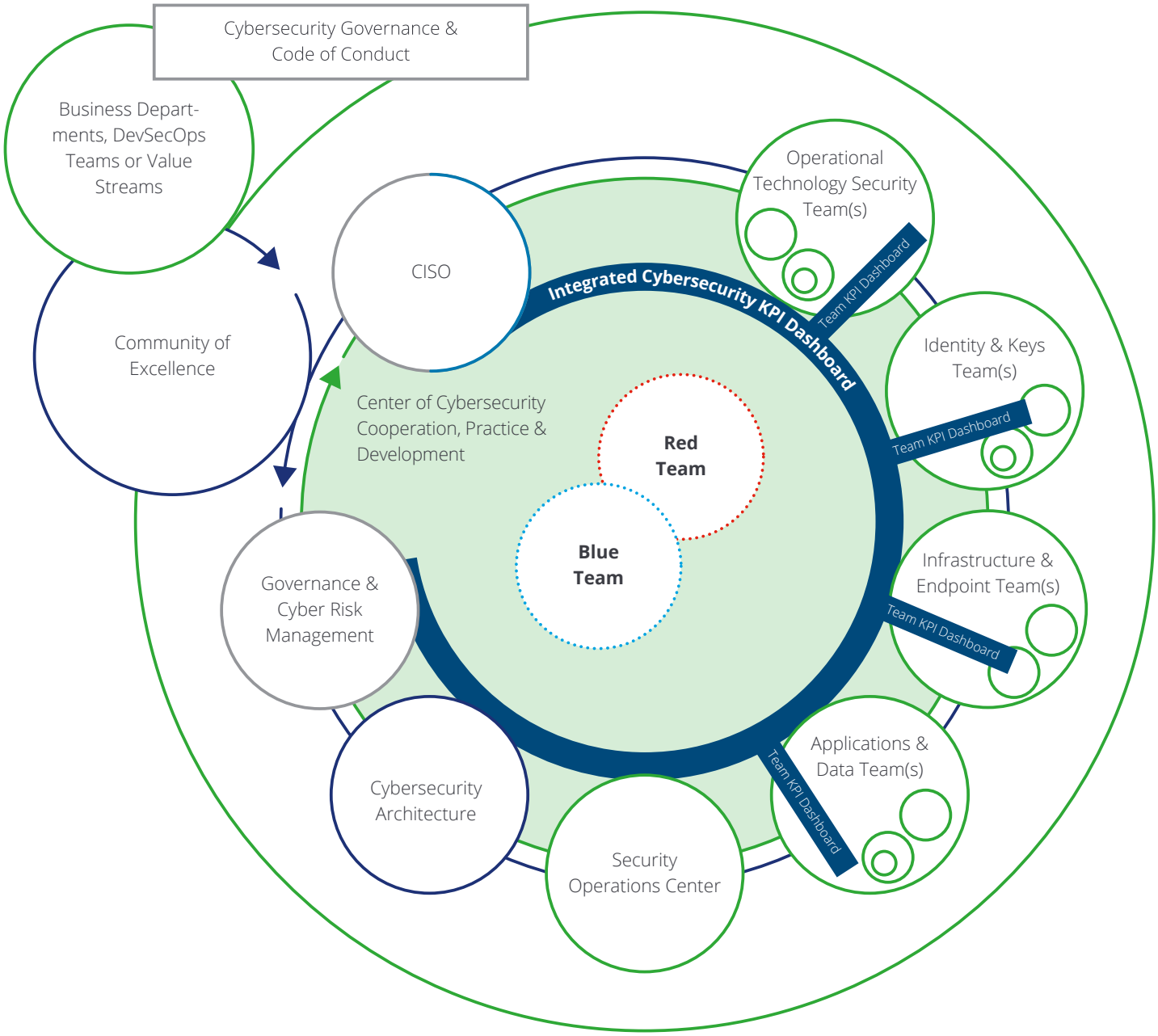


Fig. 5 – Cybernetic organization and cooperation model for CISO teams based on the Viable System Model



Cybersecurity Governance & Code of Conduct

The foundation and central point of orientation for the entire cooperation and interaction for all actors and teams of the entire company are Cybersecurity Governance & Code of Conduct. They describe the relevance and benefit of cybersecurity for the company and which quality and form of cooperation and individual behavior of all employees must be considered. This is the foundation of contribution and responsibility of each employee and thus forms the basis for autonomous and self-organized cooperation in all matters of cybersecurity in the individual and collective context.

From this starting and reference point, the individual characteristics of specific Codes of Conduct for the CSTs are derived. This mechanism shows that there is a direct link between the overarching rule and individual implementation in the context of a team agreement. This prevents the generally binding rule from degenerating into a bureaucratic, abstract superstructure without meaning or consequence. By regularly reviewing its appropriateness and applicability, Cybersecurity Governance & Code of Conduct remain lively and practical definitions that can be adapted to necessary changes.

Within the framework of regular governance sessions, the CISO and the CST Governance & Cyber Risk Management support the development process as facilitators. They ensure that all CSTs and stakeholders involved and affected have the necessary framework to apply and enforce the applicable agreements.

The role of the CISO is changing from a technical expert in his area of responsibility to a communications expert who ensures smooth cooperation between all experts.

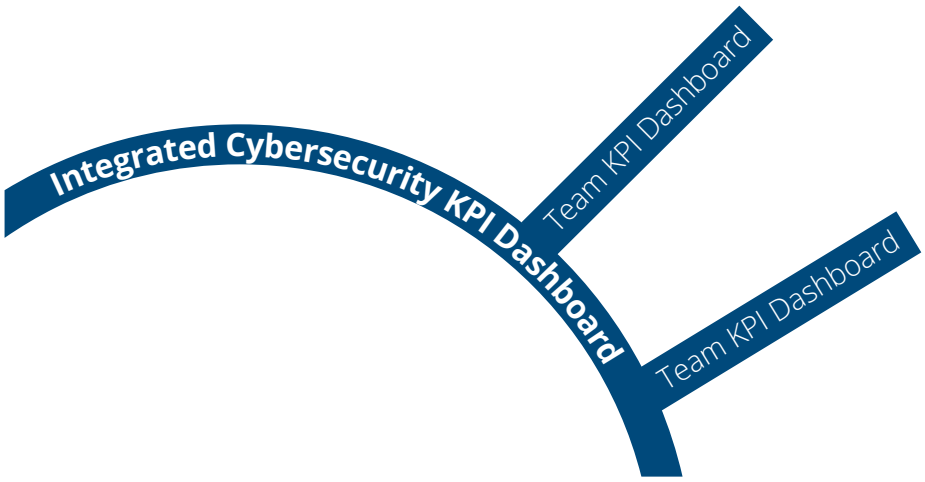
The key element of cooperation and communication between all CSTs in the CISO area are the KPI boards at team level and the aggregated ones at an overall level. In principle, all those involved and affected in the CISO area have the possibility to look at the dashboard content and to inform themselves directly about the company's cybersecurity situation. This transparency of figures, data and facts enables the CSTs to compare their individual performance to that of other teams, to support each other and promote a continuous exchange of experience and knowledge.

A peer group comparison between the CSTs can trigger friendly competition for the highest level of performance or the most advanced degree of maturity. The CISO and the CST Governance & Cyber Risk Management should make sure that this competition does not cause any dysfunctionality or conflicts.

The following presentation of the structure and content of a dashboard at the CST level should be understood as a suggestion in the context of this article. It contains recommendations and experiences of the co-authors.

When designing and configuring the CST dashboards and the information they contain, it is important to ensure that a complete integration and aggregation is maintained at the overarching recursion level of the CISO area. Only in this way, dependencies and necessary cooperation between the CSTs can be identified, communicated and coordinated at all times, for example for the analysis and processing of identified attack vectors.

Fig. 6 – KPI Dashboard



Tab. 2 – Examples of key figures

KPIs*
Level of maturity achieved vs. required
Health indicators depending on attack vectors
Hackability Score

Tab. 3 – Examples of controls

Action Backlog*	Backlog	WIP	Completed
Preventive controls	10	2	16
Protective controls	8	3	22
Corrective controls	6	2	9

* Examples merely emphatic and not complete or exhaustive

Before looking at the level of the CSTs and describing how the teams work based on the previous statements and principles, it's necessary to understand the operational application of the VSM. This will help to appreciate how CSTs can structure, organize, and communicate their strategic and operational planning and work through it.

For this, the following six building blocks[1] of the VSM are needed, from which each individual element of the CISO organization design is configured. In their combination, the building blocks define the quality and the characteristics of the contribution of the individual elements, such as a CST or, for example, the community of practice.

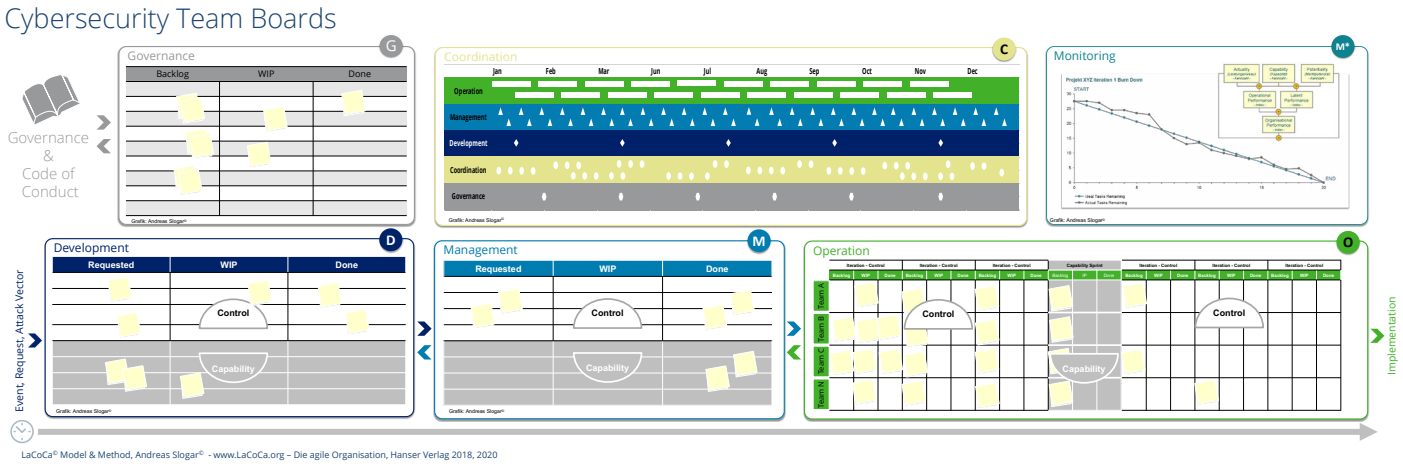
With these building blocks, the operational use cases, communicative or planning activities can be modelled in the form of self-organized cooperation. Using profiles that are published via existing Wiki or Kanban tools in the company, employees can inform themselves about the tasks of a CST, find and contact persons directly or observe the current focus and progress of the team.

Tab. 4 – Building blocks of the Viable System Model

Building Block	Definition
Operation O	• Performing an operational cybersecurity function (e.g., identity and access management, data security, threat analysis, forensic or incident response) • Providing operational work as an individual expert or in teams
Development D	• Identification and analysis of future cybersecurity developments, trends and technologies, external requirements and influences from the environment or the company on the CISO division and its services • Derivation of requisite actions to develop future required capabilities, interventions or cybersecurity strategies at corporate, CISO division, team and staff levels
Governance G	• Ensure the purpose and identity of the CISO organisation, its teams and staff • Development of and compliance with rules of cooperation and regulatory requirements through, e.g., Code of Conduct and guidelines
Management M	• Provide organisational and operational framework conditions for service delivery and development in the CISO sector • Provision of necessary resources for the delivery of operational teamwork (e.g., technological infrastructure incl. software tools and architecture, budget for investments and projects)
Coordination C	• Ensuring and further developing the cooperation of all teams within the CISO area, the corporate and the external environment • Ensure that the form, scope, quality and traceability of information between roles and teams and with their environment are functional
Monitoring M*	• Continuous analysis and control of the operational performance of all teams in the CISO series through control model (KPIs) • Accompanying all CISO teams in the self-organized derivation of action measures for the continuous development of performance on the basis of the KPI analyses

[1] Building blocks are called systems in VSM and are to be understood synonymously in this article.

Fig. 7 – Cybersecurity Team Boards



Such a profile can be configured as a set of Kanban boards that provides an integrated overview over all operational and planned activities along the aforementioned building blocks.

The profile can include the KPI dashboards already described or be published separately as an additional level of detail. The respective configuration depends on the CISO area, its CSTs and the internal and external information and cooperation needs. In any case, the design and structure of this fact sheet in the form of a cybersecurity team board must be set up so that an overarching aggregation at the next recursion level of the CISO area is possible in an automated manner.

Consistent use of Cyber Boards across all teams and communities enables seamless, transparent, and scalable orchestration of communication and collaboration among all employees, managers, stakeholders, and external partners.

All non-cybersecurity and cybersecurity teams in the company must be equally informed and trained on the necessities and benefits of IT security. For building a certain know-how and raising awareness among all employees, a Community of Excellence (CoE) is a recommended design element.

In a CoE for cybersecurity, the learning and development experts from HR can develop and implement optional and mandatory trainings for all employees. They should operate closely with CST Governance & Cyber Risk Management.

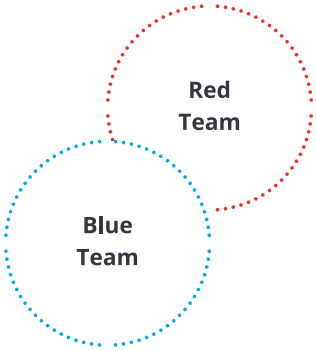
In this way, not only the continuous exchange between the CISO area and all employees is institutionalized and promoted, but also the regulatory requirements and the development of the organization-wide maturity level for dealing with cyber security issues are met.

To promote and ensure a consistent and coherent flow of information and exchange of knowledge between all CSTs, it is recommended to establish a Center of Cybersecurity Cooperation, Practice & Development (3CPD) for all employees of the CISO area. Moderated by the CISO or the CST Governance & Cyber Risk Management, the current threat situation, the individual plans of the CSTs, the results of the previous Red Team vs Blue Team maneuvers, for example, are discussed. Also, interdisciplinary cooperation is coordinated.

Within the 3CPD, different cooperation formats can be used that match the respective information and coordination needs of the CSTs and the CISO. In addition to daily stand-ups, as practiced in incremental software development, situation meetings, peer reviews or reverse presentation sessions can be planned and conducted.

A 3CPD is to be understood as an information hub to ensure the closest possible exchange of information and to prevent the formation of silos among the CSTs. In addition, the direct interaction within the framework of the 3CPD compensates for or avoids information losses and sources of misunderstanding errors through purely digital or written communication. Of course, if necessary, 3CPD can be conducted as video conferences via the usual IT tools.

The third and most relevant argument for establishing a cybersecurity 3CPD is that overarching solutions for identified attack vectors, for example, can be processed and averted in the best and fastest way possible if there is close cooperation and the smoothest possible communication between the employees of all CSTs.



Now, a final but existential element can be added that makes the essential difference to escape the unequal competition between hare and hedgehog or at least to be one step ahead of the hackers' approach. As mentioned in the beginning, an essential aspect of success is trying to put oneself in the mindset and working methods of hackers. A proven and widespread method for this is to simulate hacker attacks as realistically as possible. The employees of the CSTs form two teams.

The Red Team puts itself in the perspective of the hacker. It systematically searches for gaps at all levels and in all CIs of the IT architecture and IT infrastructure without prior notice. The Blue Team has the task of identifying attacks as well as developing and implementing effective counter-maneuvers. This form of practicing real threat scenarios is obtained from military procedures.

These maneuvers are relevant because they provide the best possible platform for consistently empowering the CSTs' staff to exercise the decision-making authority delegated to them with confidence in the event of an emergency. The smaller the delays caused by authorization queries or implementation uncertainties, the better the reaction time and efficiency of the procedure in the event of a hacker attack.

The results and findings from the maneuvers of the Red and the Blue Team should be evaluated across the board in review sessions. The Community of Excellence can use it for the development of know-how. Identified weaknesses in the IT landscape can be used by all CSTs as input for the planning and implementation of specific controls in the respective topic area.

Furthermore, time lost due to unclear procedures, contradictory or overlapping responsibilities or uncertainties in decision-making that arise during the course of a maneuver can, for example, be directly incorporated into the adaptation of governance and the Code of Conduct at the level of the CISO unit or the individual CSTs.

Conclusion

The design of a CISO organizational model with the help of the principles and tools of cybernetics used here in an excerpted and simplified form enables the representation of the organizational chart of existing CSTs. It also points out possible forms of cooperation, the most important communication channels and content as well as the integration of the entire CISO area into the corporate environment of the non-cybersecurity areas.

The presentations in this article cannot be fully comprehensive. Nevertheless, the impulses are certainly suitable for questioning the existing, classic and very widespread understanding of the design and cooperation model of a CISO sector and developing it further. CISO units need to use of the cleverness of the hedgehog in the race against hackers, instead of spending more and more effort and energy, like the hare, and ultimately fall into despair because of oneself and the challenges of cybersecurity.

The antifragile Web3: a cybernetical view

Yip Thy-Diep Ta | Unit Network

Yip Thy-Diep Ta is a cofounder at Unit Network, a blockchain for token economy. Through her initiatives DLT-Talents, Unit Masters, and H.E.R. Dao, she provides free educational programs and scholarship opportunities to promote equity in Web3. Yip is a cofounder at the Balanced Being cooperative, which provides mindfulness & compassion trainings. She is the author of the book "Beautiful Brains change tomorrow... today", and has received several awards as one of the most influential women in Blockchain. Previously, she was a consultant at McKinsey & Co.

One of the most important challenges being faced today is how to deal with the side effects of globalization and connectivity. As the world becomes ever more unpredictable, how can we face the ever-increasing frequency of Black Swan events? We propose a cybernetic approach, shifting from linear, cause-and-effect models to circular models that accept interdependent relationships.

By viewing ourselves as participants in future ecosystems, we can capture our own impacts and incorporate this information into the continuous evolution of antifragile systems. These systems will be shaped by the decision-making of individual human beings, who themselves exist as living systems of continuous feedback and growth. They themselves are a subset of nature. We propose mindfulness as a critical competency for building systemic antifragility.

One interesting use case is Web3, the Internet of Value. Digital assets (cryptocurrencies), the underlying distributed ledger technologies (blockchains), and the new modes of collaboration (Decentralized Autonomous Organizations and Transient Antifragile Organisms) create a fertile ground for the emergence of antifragile systems.

What do you do in a world you don't understand?

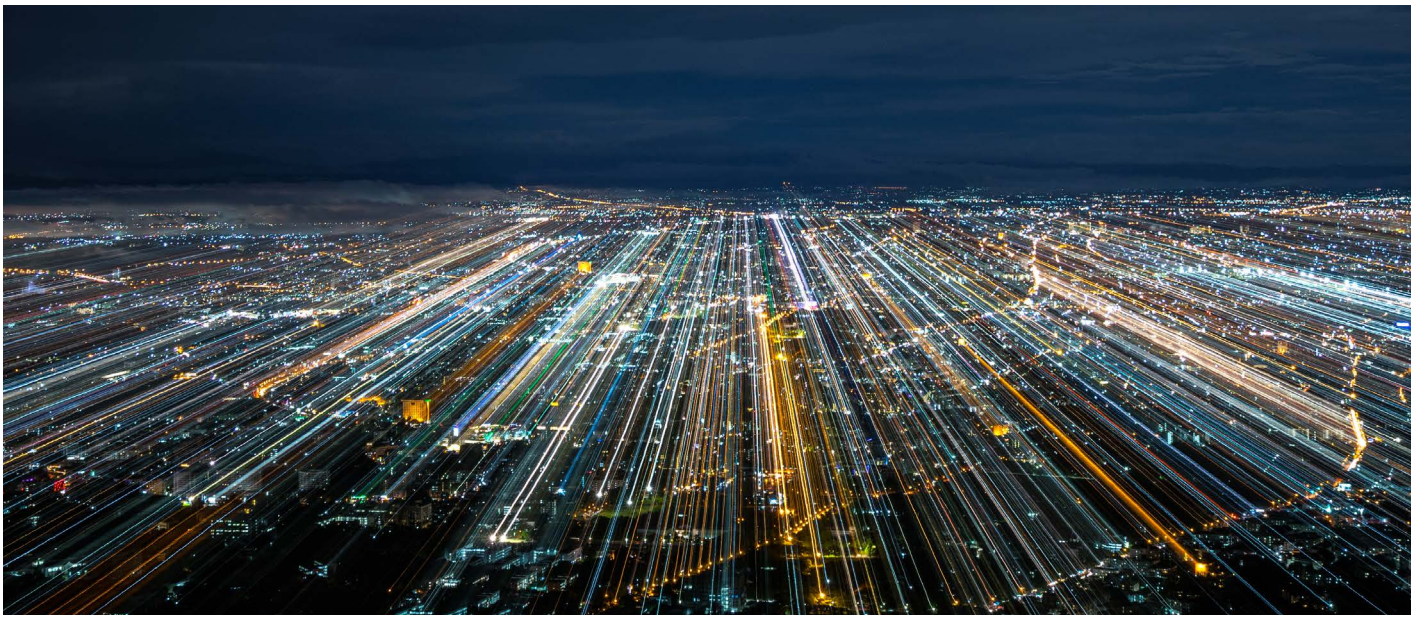
Technological progress and globalization – for all the benefits they have brought – have resulted in complex systems full of interdependencies that become increasingly difficult to identify as systems grow in size. Unnoticed, these interdependencies lead to chains of unforeseen effects that can assume catastrophic proportions. In the future, we will be increasingly beset by so-called Black Swans – unpredictable, rare events with potentially catastrophic consequences.

Rather than relying on our ability to recognize and account for all interdependencies in a system of global scale, it is appopriate to assess the vulnerability to these catastrophic Black Swan events and their impacts, and build systems in which volatility is more enrichment than danger. Ultimately, what matters is sensitivity and preparedness to these unpredictable, rare events, not the likelihood of their occurrence.

Antifragility is a property attributed to a situation in which an object or person experiences a gain or otherwise defined enrichment that exceeds potential losses in response to volatility. In his book "Antifragile: Things That Gain from Disorder" statistician and former stock market trader Nassim Taleb posits that it is impossible to predict the likelihood of the next Black Swan and that, against this backdrop, the optimal strategy for action is to position oneself for the best possible outcome when these events occur.

In antifragile systems, we account for the occurrence of low-probability, extreme events in such a way that the rare payoff that we do receive will compensate for the cost of exposing ourselves to these events. Ideally, the utility function of our action strategy follows a convex course similar to a smiley, in which events with the lowest probability have the greatest positive impact on our system. Larger deviations from the expected mean lead to higher gains in such a system. Ideally, this takes the form of convex response curves in which the lowest probability events have the highest positive impact. Antifragility goes beyond robustness, in the way that antifragile entities do not only resist shocks, they improve with every shock.

Taleb proposes a bimodal strategy that limits the downside in case of rare negative Black Swans and maximizes the upside in case of rare and extremely positive events. This provides robustness in the case of extreme negative shocks and optimizes exposure to beneficial situations (positive Black Swans).



To counter the risk of catastrophic events, negative outcomes with small losses are encouraged as learning opportunities and contribute to the overall health of the system. This leads to the development of a systematic response strategy that positively feeds back into itself with each additional deviation from target values. The more errors occur, the faster the system improves. Small weaknesses are discovered which, if not corrected, can lead to greater damage over time. Errors are therefore not a problem, but an asset, as they reduce the occurrence of larger errors with serious consequences. This form of continuous improvement does not eliminate Black Swans or make them more predictable, but it does improve the chances of survival should a Black Swan appear.

Once it is ensured that the risk of ruin is reduced as best as possible, any action that results in more options being available for exposure in terms of positive outcomes in terms of organizational goals is a profitable one, provided that the cost of securing the options is negligible relative to potential payoffs. In summary, we provide antifragility to a system by:

- Best possible reduction of the risk of complete ruin
- Developing a systemic response strategy that feeds back on itself by encouraging sizable failures
- Increasing optionality with reference to events that enable high payoffs

To develop a response strategy for a given system, all persons must be included as an essential part of that system. The human actors act, the system responds, which in turn influences the human actors and their next responses – all in a constant circular feedback loop. This is the realm of second-order cybernetics. When the response strategy follows the principles of antifragility, it becomes a system of continuous improvement between the components of the system.

A cybernetical view on impact and responsibility

In second-order cybernetics, as defined by Heinz von Foerster, the observer sees himself as an actor in the system he observes. In this view, the objective independence of the subject from the system is suspended: All actions of the participants are part of the internal feedback process that determines how the system unfolds through itself. None of the observing actors can absolve themselves of some responsibility for the observed outcomes, whether positive or negative. The role of the human actors is to choose their interpretation of the information perceived from the system and their response strategies.

As Viktor Frankl wrote in "Man's Search for Meaning", our responsibility lies in our ability to choose a response to a given situation – and this response includes the way in which we conceive of the situation itself. Our responsibility is to increase our accountability, that is, to increase the number of response options. We can do this by, for example, improving the skill of perception and becoming aware of the effect of our actions, or our participation in the system.

In the following, let's have a look on mindfulness as the critical skill with which the feedback loop of actors will be improved continuously by sharpening subjective perception through an expanded information base, thus increasing the system's antifragility.

Mindfulness: a missing link in the world of antifragility

In the 70s, the researcher Jon Kabat Zinn introduced mindfulness to the Western scientific world. He defined it as "awareness that arises through paying attention, on purpose, in the present moment, non-judgmentally" (Moore, 2019).

Mindfulness is an important skill for gaining better self-awareness and identifying blind spots in decision-making. This is done by expanding the number of sources of information from intellectual, fact-based understanding of a situation to emotional intelligence and embodied intuition.

In recent years, organizations have begun to implement mindfulness training to improve overall organizational performance by expanding the competencies for (emotional) self-regulation of the actors in their systems. Mindful employees make decisions differently and communicate better with themselves and others.

This training leads to an increased awareness of internal reactions which increases optionality in decision-making. Mindfulness training typically includes body scans to understand the embodied impact of thoughts and emotions, and exercises that help develop a more granular vocabulary of the emotional landscape.

Exercises to increase compassion aim to cultivate an emotional response that can be acted upon in the interest of another actor's well-being rather than out of empathic distress. Compassion, when applied to the self, for example, increases motivation to continue to engage with the underlying object of learning despite failures (Breines & Chen, 2012). Compassionate communication involves the practice of examining one's own internal thought processes and emotional pain responses rooted in the body as one's pre-programmed response to an external trigger and choosing a response that is consistent with one's understanding of what is the responsible solution for the stakeholders involved, including oneself.

One of the main benefits of cultivating a consistent practice of mindfulness and compassion is that it raises awareness of the impermanence of the nature of things, thus training practitioners to face the erratic Black Swan world of perpetual change with ease and grace. It prepares decision-makers to face the Black Swan's stormy eye with equanimity, and keeping a calm mind in turbulent times.

Neuroscientists, while still at the early stages of their research, have shown that practicing different styles of mindfulness exercises affects brain areas that are related to perception, awareness, pain tolerance, emotional regulation, introspection, complex thinking, and the sense of self. Researchers have observed changes in gray matter density in different brain regions, such as the Anterior Cingulate Cortex (ACC), an area associated with self-regulation and the ability to purposefully direct attention, and in the Hippocampus, a part of the limbic system associated with emotions and memory (Congleton/Hoelzel/Lazar, 2015).

Mindfulness and compassion in communication not only impact the relationships, creativity, and performance of individual participant-actors, but are indispensable pillars for feedback loops in antifragile cybernetic systems.

Internet of Value, Token Economy and DAO

Web3, commonly referred to as the Internet of Value, is the next phase of the Internet. It follows in the footsteps of Web1, the Internet of Information, and Web2, the Internet of Communication, which have significantly reduced the cost of information on the one hand and the cost of global communication on the other.

The Internet of Value is an important enabler of the antifragile cybernetic systems of the future because it empowers people to independently create new forms of value. The ability to ascribe digital value to all manner of endeavors, distribute that value, and coordinate contributions

to value creation in a nearly costless way through permission-free technology strengthens the radical reduction of costs in globalized economic exchange and creates unprecedented opportunities for greater participation in and reduction of wealth inequality throughout the economy.

At the time of writing the Web3 market is valued at around 1 trillion USD, a mere 1 percent of the global equities market. As of July 2022, the top ten most popular applications had on average only 500,000 unique monthly users (DappRadar, July 2022). While still in its nascent stage, this industry has the potential to massively increase in the number of people who can access the benefits of an economy based on free, open, and voluntary exchange. According to the wealth manager Wells Fargo, "Digital assets are a transformative innovation on par with the internet, cars, and electricity" (Wells Fargo, 2022).

The wealth generation potential of this industry has also not been lost on hackers, who are responsible for the theft of 14.5 billion USD worth of crypto assets since 2011. In the first half of 2022 alone, more than 2.5 billion USD worth of digital assets were stolen from the largest ten decentralized finance projects – projects which represent one of the first major use cases of the Internet of Value (CoinDesk).

In Web3, value is inscribed into digital containers called tokens that can be sent instantaneously and immediately from user to user (peer-to-peer) without the need for a centralized intermediary. In the so-called Token Economy, there are no limits to the variety of values that can be represented, modeled, and exchanged. Both transactions and the actions of decision-makers are transparently visible to the entire ecosystem.

These tokenized economies build on the Web3 Internet of Value and can reduce the prevailing inequality in wealth by enabling all participants to benefit from the value they create. For example, by receiving a token allocation in the collaborative project to whose value creation they have contributed in a visible and measurable way through their participation in the first place. This enables actors to create systems in which many more people can have "skin in the game" by becoming a stakeholder of any venture they contribute to. In Web3, thanks to the technological architecture and the values that can be represented by digital tokens, the impact and value contribution of the entrepreneurial actors can be directly connected.

Web3 is a system in which accountability is transformed from an active to a passive form of reporting: at any time, any actor is able to view all value transactions conducted in the ecosystem and on the blockchain ("on-chain"). The hidden philosophy of action in such systems is underpinned by the inference "I know that you know that I know," as transparency is by design encoded in the system. This transparency improves decision-making by reducing prevailing information asymmetries.

One of the signature innovations of Web3 is the DAO, the Decentralized Autonomous Organization. DAOs can be seen as cooperatives owned and managed collectively by their members, taking advantage of blockchain technology for coordinated action and decision-making. In DAOs, decision-making authority and administration of the treasury is distributed among stakeholders rather than being centralized in the hands of a few managers. As of July 2022, the decentralized cryptocurrency exchange UniSwap, for example, holds 4 billion USD worth of crypto assets in their treasury governed by a community of 350,000 token-holders and their delegates, who propose and vote on upgrades to the project. Since its inception in August 2021, the UniSwap DAO members have voted on 89 proposals with participation of a total of 8,300 voters and a proposal success rate of 45 percent (DeepDao Database, July 2022). The outcomes of proposals and the flow of value into and out of the treasuries can be reviewed via free online tools that enable any stakeholder to search for real-time and historical information about transactions that happened on the blockchain.

The next step in Web3: from DAOs to TAOs

The introduction of cybernetic principles, mindfulness and compassion in communication is the next step in the evolution of the Web3 ecosystem. DAOs become TAOs: Transient Antifragile Organisms. When the cybernetic view is applied to the nature of collaboration, the DAO becomes a living organism, an entity where the whole is greater than the sum of its parts. TAOs are designed to evolve and scale rapidly and to reinvent themselves again and again. TAOs are not afraid of hacking because they have developed processes to identify their vulnerabilities and reduce the risk of complete elimination. The TAO is distinguished by three key characteristics:

- Robustness: ability to recognize and reduce the risk of elimination
- Adaptability: ability to let go of the fear of failure
- Growth: ability to capitalize on the volatility of events

As a transient organism, the TAO is an entity that by design is of impermanent nature, and will be in existence only as long as it effectively serves the purpose for which it was brought to life. In the TAO, the participant-actor is the mechanism that maintains balance in the organism by detecting changes in conditions and adjusting itself accordingly in the iterative feedback loop.

Decision-makers within TAOs are trained in the disciplines of cybernetics, mindfulness and compassion. They know how to contemplate impermanence, and know that despite the risk of ruin, the knowledge that has been accumulated within the actors of the TAO will not be lost to humanity. Embracing volatility as an opportunity to learn, the TAO is well equipped to look into the eye of the storm with compassionate curiosity instead of paralyzing fear – and will magnify the historic contribution of the Token Economy to reduce prevailing wealth inequality in today's world.

References

- Baydakova, A. (2022, July 27). DeFi Has Become Crypto Crime's Main Arena, Crystal Blockchain Says. CoinDesk. https://www.coindesk.com/business/2022/07/27/defi-has-become-crypto-crimes-main-arena-crystal-blockchain-says/
- Breines, J. G., & Chen, S. (2012). Self-Compassion Increases Self-Improvement Motivation. Personality and Social Psychology Bulletin, 38(9), 1133–1143.
- Congleton, C., Hölzel, B., Lazar, S. (2015). Mindfulness Can Literally Change Your Brain (Digest Summary). Harvard Business Review.
- Foerster, H. von (1995 [1975]). Kybernethik. Berlin: Merve Verlag.
- Moore, C. (2019, April 9). What Is Mindfulness? Definition + Benefits (Incl. Psychology). PositivePsychology. Retrieved July 25, 2022, from https://positivepsychology.com/what-is-mindfulness/
- Organizations (2022). DeepDAO. Retrieved July 25, 2022, from https://deepdao.io/organizations
- Taleb, N. N. (2012). Antifragile: Things that gain from disorder. New York: Random House.
- Top Blockchain Dapps (2022). DappRadar. Retrieved July 27, 2022, from https://dappradar.com/rankings/1
- Wells Fargo (2022, August). Digital Assets – A World of Possibilities. Wells Fargo Advisors. https://www.wellsfargoadvisors.com/research-analysis/reports/cryptocurrency/digital-assets.htm

List of authors

Hacking protection – a never ending competition inside of companies?
Dr. Karsten Nohl is a hacking expert and founder of Autobahn Security in Berlin. Karsten creates awareness for cybersecurity – through hacking research and consulting. He is particularly fascinated by the trade-off between security and innovation.

Cybersecurity and cybernetics
Dr. Ralf Schneider has been Group CIO of Allianz SE since 2010 and is responsible for IT Governance, Strategy and Security globally. Prior to that, he was Board Member for IT of Allianz Managed Operations & Services SE (2010–2016) and CIO of Allianz Germany (2006–2010). After his studies in mathematics and a PhD in computer science, he started at Allianz in 1995. For more than 25 years, he has held leading positions in IT, including department head of Information Systems Sales and department head of e-Business and Project Controlling Germany. In addition, he is a mandate holder of several cyber security organizations such as Cyber Security Sharing & Analytics e.V., the German Cyber Security Organization and the Digital Society Institute at ESMT.

What is cybernetics?
Prof. Dr. Fredmund Malik is a recognized management expert and chairman of management and advisory boards in business corporations. He is a pioneer of management cybernetics and complexity management. He was a member of the board of directors of the Institute of Business Administration and, in parallel, of the St. Gallen Management Center since 1977. He is the author of more than 15 books. His book "Führen Leisten Leben" (Lead Perform Live) was voted among the 100 best business books of all time. In 2018, he received the Life Achievement Award, the highest honor in the German management education system.

Design and management of agile cybersecurity organizations
Andreas Slogar has worked in more than 20 countries, the USA, Europe, the Middle East and Africa and has built up extensive experience in strategic and operational management work, including as CIO. As an expert, Slogar specializes in transforming entire companies into a adaptable collaboration state and is the author of various articles, podcasts and the book "The agile organization" (Hanser Publisher, 2018, 2020 – German).

The antifragile Web3: a cybernetical view
Yip Thy-Diep Ta is a cofounder at Unit Network, a blockchain for token economy. Through her initiatives DLT-Talents, Unit Masters, and H.E.R. Dao, she provides free educational programs and scholarship opportunities to promote equity in Web3. Yip is a cofounder at the Balanced Being cooperative, which provides mindfulness & compassions training. She is the author of the book “Beautiful Brains change tomorrow... today”; and has received several awards as one of the most influential women in Blockchain. Previously, she was a consultant at McKinsey & Co.

Contacts

Nils Dennstedt
Partner
Sector Lead Insurance
Tel: +49 40 32080 4463
ndennstedt@deloitte.de

Marius von Spreti
Partner
Cyber
Tel: +49 89 29036 5999
mvonspreti@deloitte.de

Andreas Slogar
Senior Manager
Agile Business Transformation
Tel: +49 151 58077936
aslogar@deloitte.de

Deloitte.

Issue 11/2022