AGENDA

FUTURE CYBER THREAT ANALYSIS WORKSHOP
@
CODE CONFERENCE 2021
BUNDESWEHR UNIVERSITY MUNICH

Aim and Scope

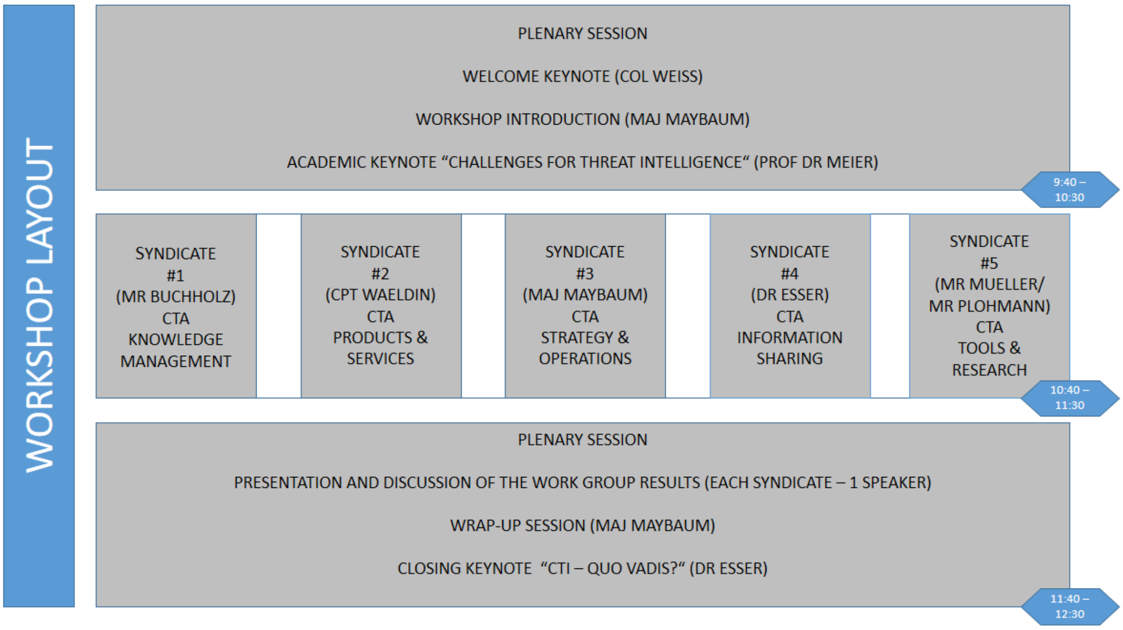
In this workshop conducted by Bundeswehr Cyber Security Centre (ZCSBw) we will reflect state-of-the-art techniques within the field of Cyber Threat Analysis (CTA) and explore current challenges both from a practitioner's view as well as from an academic perspective. We aim to identify future fields of research and development by identifying current shortfalls such as technology gaps, implementation problems, information sharing and interoperability issues as well as challenges in the field of cyber threat knowledge management in order to derive future requirements for the military as well as for the public and the private sector, and to inspire and foster capability development and enhancement in this discipline.

Format and Planned Activities

The workshop will have five working groups, each syndicate working on a specific question about the subject. As an introduction, the workshop will start with a plenary session having an academic keynote speech to set the scene for the working groups. The results of the syndicate work will be presented in a wrap up plenary session, concluded by a keynote focusing on future development and the way ahead. For both keynotes and syndicates, we invited academic partners (Gartner, Fraunhofer FKIE) contributing as subject matter experts. In addition, the entire workshop will be academically assisted by Prof. Dr. Harald Baier from CODE research institute.

Tentative Agenda

The workshop divides into five sessions:



WORKSHOP LAYOUT

PLENARY SESSION

WELCOME KEYNOTE (COL WEISS)

WORKSHOP INTRODUCTION (MAJ MAYBAUM)

ACADEMIC KEYNOTE "CHALLENGES FOR THREAT INTELLIGENCE" (PROF DR MEIER)

9:40 – 10:30

SYNDICATE #1 (MR BUCHHOLZ) CTA KNOWLEDGE MANAGEMENT

SYNDICATE #2 (CPT WAELDIN) CTA PRODUCTS & SERVICES

SYNDICATE #3 (MAJ MAYBAUM) CTA STRATEGY & OPERATIONS

SYNDICATE #4 (DR ESSER) CTA INFORMATION SHARING

SYNDICATE #5 (MR MUELLER/ MR PLOHMANN) CTA TOOLS & RESEARCH

10:40 – 11:30

PLENARY SESSION

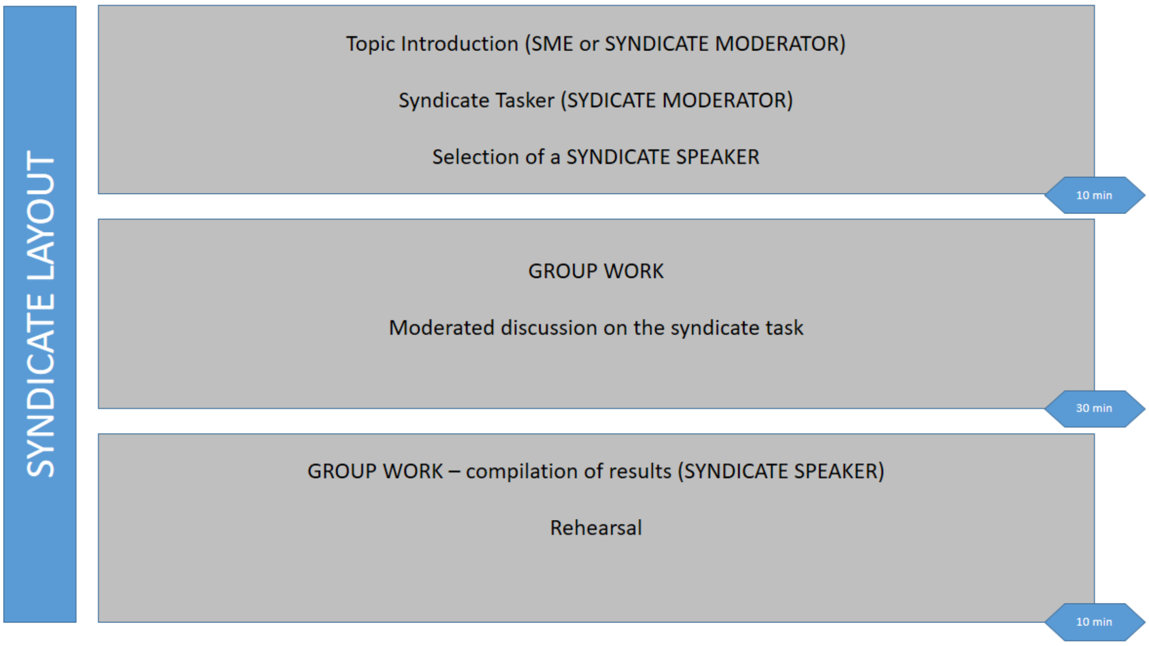
PRESENTATION AND DISCUSSION OF THE WORK GROUP RESULTS (EACH SYNDICATE – 1 SPEAKER)

WRAP-UP SESSION (MAJ MAYBAUM)

CLOSING KEYNOTE "CTI – QUO VADIS?" (DR ESSER)

11:40 – 12:30

For group work in the syndicate, the group will divide into five syndicates to work on different aspects of future challenges for CTA. The syndicates will open with a tasker and a motivation talk reflecting the current state-of-the-art as well as identified needs for research and development. The group will then be given time to work on the tasking and prepare a short findings report to be presented in the concluding plenary session.



SYNDICATE LAYOUT

Topic Introduction (SME or SYNDICATE MODERATOR)

Syndicate Tasker (SYDICATE MODERATOR)

Selection of a SYNDICATE SPEAKER

10 min

GROUP WORK

Moderated discussion on the syndicate task

30 min

GROUP WORK – compilation of results (SYNDICATE SPEAKER)

Rehearsal

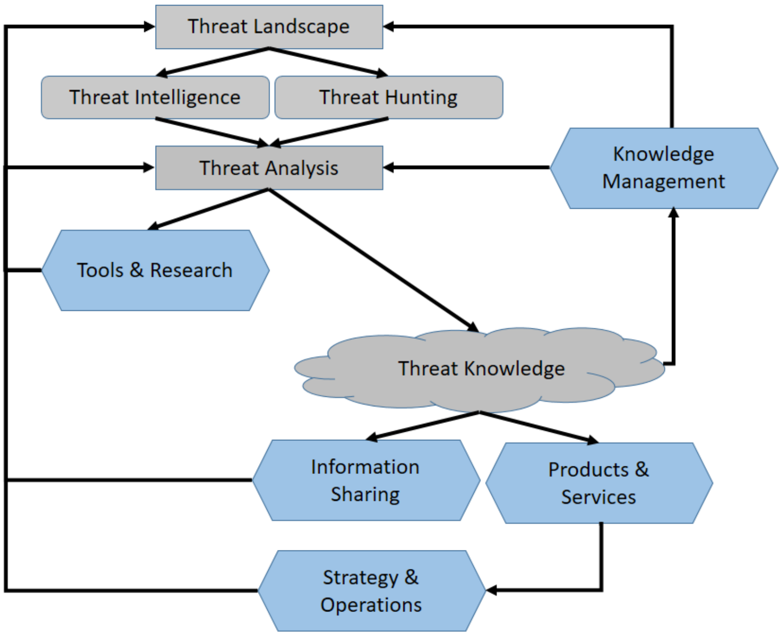
10 min

Abstracts for the syndicates are attached as Annex A, short biographies of the workshop organizers and speakers are attached as Annex B; alternate/additional moderators/speakers may be added as applicable.

Annex A – Syndicate Agendas

SCOPE

Threat Analysis is a core function within the scope of business risk mitigation. Cyber Threat analysis (CTA) is a discipline within that field focusing on threats from and within the cyber domain – the so-called cyber threat landscape. Information on cyber threats are usually gathered in an intelligence process collecting significant data from available sources and compiling them into an integrated threat picture, nowadays more and more amended by findings from a hunting process within the own organization. This entire process aims to develop and maintain an up-to-date knowledge hub from which products and services can be derived to advise and support business operations as well as strategy development. An appropriate knowledge management as well as sharing of threat knowledge with partners helps to continuously improve this process, also fostering research and the development of new tools supporting the analysis are important in that context.



The syndicates presented in this workshop focus on these aims[1]: the first syndicate we will look deeper into knowledge management in the context of cyber threat analysis since this function is key for any successful contribution in term of gained value – and this knowledge must be made operationable. Therefore, the second syndicate will explore state-of-the-art advisories and discuss how threat knowledge can be presented most efficiently to business operations and strategy development, the requirements of the executive level will be analysed in syndicate #3.

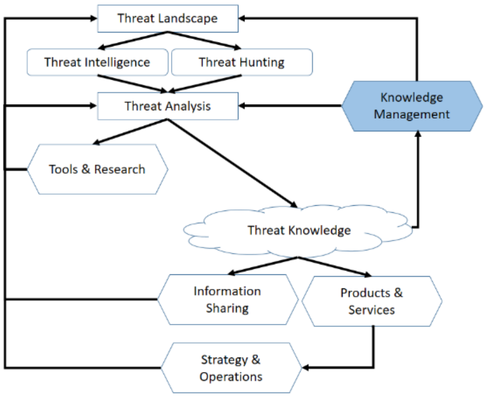
Requirements of information sharing as well as aspects of tool development and future fields of research will be elaborated in two optional syndicates or will be integrated into the discussions within the first three working groups. Information sharing between partners is a necessary key enabler in this discipline since the number and quality of threats evolving has reached a threat level that a single business or organization cannot handle anymore just relying on own capacities. Even more important is research and the development of tools; therefore, we intend to offer a hands-on exercise offering practical insight into state-of-the-art tool application within the analysis process and discuss which future requirements could be addressed on the toolbox side.[2]

[1] Highlighted in blue color in the figure above.

[2] The practical part will be conducted in cooperation with our partner Fraunhofer FKIE.

SYNDICATE #1	CYBER THREAT ANALYSIS – KNOWLEDGE MANAGEMENT
MODERATOR & TOPIC KEYNOTE	MR JAN-CHRISTOPH BUCHHOLZ (ZCSBw)
PARTICIPANTS	MIN 5 – MAX 20

The main challenge all threat analysts have to face nowadays is handling the masses of information they see themselves exposed to as well as deriving and developing knowledge form these feeds – and the even more emerging problem of maintaining and managing this knowledge within their organization. In a deeply technical field filled overwhelmingly with people from a technical background, knowledge management is mostly understood as keeping technical indicators and relevant meta data accessible and searchable.



Vendors provide Gigabytes of raw threat information assembled by huge sensor networks and intelligence services active around the globe. By now, numerous platforms for storing and exchanging technical information on threats have been proposed and standards such as TAXI or STIX have been defined and are used by state-of-the-art platforms to automate the handling of mass data transfer and analysis.

While automation frees human resources from the burden of easily repeatable tasks, human thought processes about highly specific topics on the other hand can be much less oriented along formal categories of IOCs or TTPs, but far more unstructured, unfinished, or not yet verified instead. Still their results, even in a state before reporting, are worth keeping beyond the personal capability of the mind of a single threat analyst along with the primary sources they derived from as they make future reporting faster by preventing the need of redoing all previous steps of information gathering and sorting. Additionally the information should never be bound to a single person, but easily transferable into the analytic work of others.

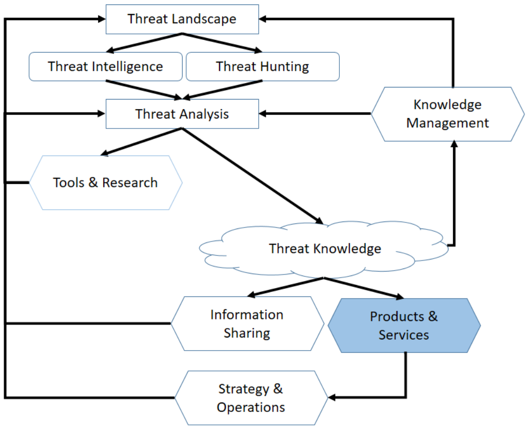
Knowledge management beyond relatively short-lived technical indicators is essential to prevent most of the impact of experienced analysts leaving their role and enables a much faster and a more efficient training of new analyst and an increasing maturity of the CTA program overall. While traditional database solutions require a predefined structure and data format, CTA queries emphasize links between diverse kinds of information over single data entries with changing starting points depending on future hypothesizes.

Therefore, Syndicate #1 will focus on possible techniques to provide a knowledge management for (partially) analysed information and unstructured texts not focusing on automating human analytic work, but on supporting the underlying processes, documentation and reporting.

SYNDICATE #2	CYBER THREAT ANALYSIS – PRODUCTS & SERVICES
MODERATOR	CAPTAIN PATRIK WAELDIN (ZCSBw)
TOPIC KEYNOTE	MAJOR ALEXANDER BAGUS (JIC)
PARTICIPANTS	MIN 5 – MAX 20

This syndicate looks into products a mature CTA process can and should provide. Threat analysis by its nature is a tool designed to help mitigate risk. In its core function, the identification and evaluation of threats is a requirement to ensure successful operations of a business or of an organization.

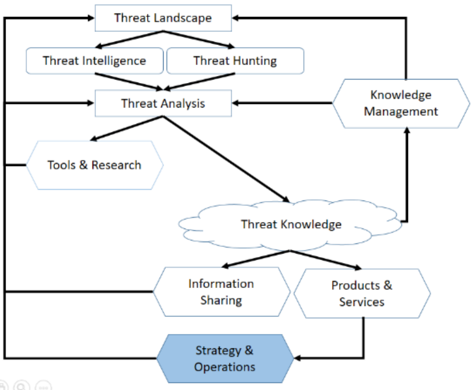
Currently, the main task of deliverable production for a CTA is to provide technical advisories, summarizing threat knowledge for both the IT security management as well as for the executive level of an organization, different of course in content and objective.



Whereas an advisory for an IT security expert can be mostly concise and straight to the (technical) point, especially consequences for business operations and even more for the strategic level often require a broader scope, analytic background and – depending on the case and business – often also a political perspective.

The main questions we therefore deal with in Syndicate #2 will be the discussion on products CTA produces to empower the strategic decision making process and to contribute to risk mitigation within current business operations. In this respect, the CTA products we elaborate on should create a link between the tactical/technical level, the operational levels and the strategic level. We will explore – in a bottom up approach – which information will be required by a CISO (business/organization/military) and/or an intelligence branch and which products are usefully for operational personnel like incident response, SIEM or FW/IDS/IPS operators. We will discuss stakeholders' priorities, content, layout, frequency and number of products as well as workflows – from a CTA practitioner's perspective.

SYNDICATE #3	CYBER THREAT ANALYSIS – STRATEGY & OPERATIONS
MODERATOR & TOPIC KEYNOTE	MAJOR MARKUS MAYBAUM (ZCSBw)
PARTICIPANTS	MIN 5 – MAX 20



Though not being a brand new discipline, CTA nowadays is often still believed to be an entirely technical discipline within the scope of the cyber security process of an organization. Especially at executive and management level, risks arising from the cyber threat landscape are often not seen or at least underestimated. Cybercrime as one of the most significant financial risks to a business as well as state-actors' using cyber means to achieve strategic or operational objectives are meanwhile commonly known – the more interesting it is to see that only a small minority of organizations have implemented CTA mechanisms within their strategic and operational planning entities.

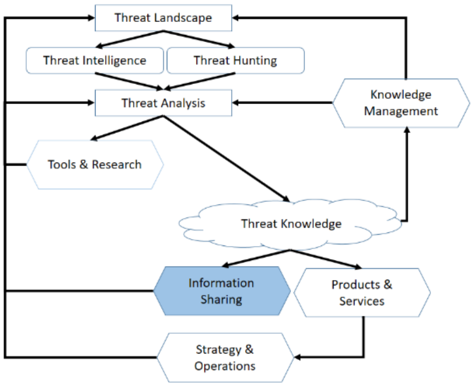
Many decision makers deem to believe that cyber threats is primarily a problem of their IT security organization ignoring the evidential situation that the increase of global economy loss due to cybercrime has reached a level comparable to the gross national product of smaller states.

Syndicate #3 will look into strategy development and business operations to raise the awareness of cyber threats and their potential impacts to an organization – or even to a state. In a top-down-approach we will edge out the key objectives that need to be evaluated in terms of viable threats aiming to ensure appropriate precautions measures and built-in resilience within processes of common joint strategic and operational planning – in business as well as in governmental entities, also focusing on the military. We will work along well-known models and international best practices to identify necessary adaptations and amendments to operationalize available threat knowledge – from the known knowns to the unknown unknowns.

Based on this analysis, we will raise the question, how CTA can be better integrated into business processes. We will look into methods of operations research and focus on requirements the executive level has and what answers CTA can provide in this context to improve risk mitigation in future. We will also conclude, what capabilities we need, derive suggestions for new fields of research and/or tool development as well as possible ways ahead in terms of mitigation with regards to structural and organizational shortfalls, and administrative gaps.

SYNDICATE #4	CYBER THREAT ANALYSIS – INFORMATION SHARING
MODERATOR	DR. BERND ESSER (GARTNER)
TOPIC KEYNOTE	LTC CHRISTOPH KUEHN (ZCSBw)
PARTICIPANTS	MIN 5 – MAX 20

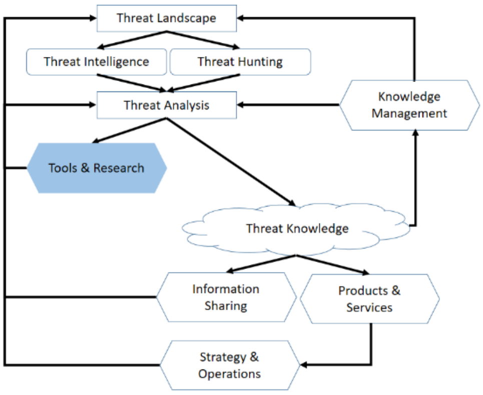
Any mature CTA process needs to rely on external intelligence. In most cases, this intelligence is obtained either from the commercial market, gathered from open sources or received from partners through an information sharing network. Information obtained from the commercial market nowadays is one of the most significant sources of information since a specialized industry developed the demand for reliable threat information as their business model and offers dedicated products and services to any paying customer sufficing their needs for an adequate level of security.



However, commercial solutions mostly focus on the broad markets, and mature products for more specific needs are rare and expensive. One option for an organization with specific needs might be to development of an own threat hunting capability – expensive as well and not an easy task to do since expertise and personnel having the necessary qualification and experience are rare as well. Consequently, only a minority of organizations can afford that. Threat hunting can be outsourced to a joint venture or another external service provider, still the core problem maintains.

Another viable option therefore is another form of burden sharing: sharing threat information. This syndicate will look into state-of-the-art information sharing regimes and discuss their value as well as their limitations from a technical as well as from a business and legal perspective. We will try to identify shortcomings in the current existing networks and try to envision new concepts and future solutions for these gaps. We want to draft requirements for future threat information sharing with a special focus on current limitations and to stimulate a proposal for decision makers on how the concept of information sharing can be improved for a true value add and common benefit of all.

SYNDICATE #5	CYBER THREAT ANALYSIS – TOOLS & RESEARCH
MODERATORS	ROBERT MUELLER / DANIEL PLOHMANN (FRAUNHOFER FKIE)
PARTICIPANTS	MIN 5 – MAX 12



CTA is a complex and highly dynamic discipline that requires continuous adaptation to the advancement of tools and techniques used from an adversary. The permanent changes of the threat landscape forces analysts to always keep pace with the development of malware and attach techniques to stay competitive. In this respect, CTA is an active key player in the arms race between the actors in cyberspace and forced to gain and maintain the balance of power, which requires a steady improvement of available means and methods.

This syndicate focusses on research in the field of CTA tools. We will practically demonstrate a state-of-the-art analysis process highlighting the challenges at a practical example. For this, we will introduce a set of non-commercial tools as a result from current research in the field of threat analysis: a non-commercial tool for rapid identification and actionable context as well as a novel CTA parser tool. We will offer syndicate participants to analyze a case hands-on using those tools and to discuss the tools performance and usability in a real-world scenario context as well as from a future threat perspective. Based on these findings, we intend to derive requirements for next generation CTA tools as well as challenges for new research projects.

IMPORTANT NOTE:

This is NOT a deep technical syndicate, however: for the hands-on part of this syndicate, it would be beneficial if the participants have a practical CTA background or at least some first practical experience within core cyber security disciplines such as Digital Forensics, Malware Analysis, Penetration Testing, etc.

Annex B – Short Biographies

Lead Author and Moderator:

Major Markus Maybaum (ZCSBw – Haed of Cyber Threat Analysis)

Markus Maybaum is a German Air Force officer with more than 20 years of professional experience in the field of IT and cyber security. He worked in several different national and international management, leadership and expert positions focusing on arms control, malware analysis, penetration testing, and cyber threat intelligence; at present, Markus is heading Cyber Threat Analysis at the German Military Cyber Security Operations Centre in Euskirchen, Germany. He is also an alumnus of various senior level educational institutes such as the US George C. Marshall European Center for Security Studies or the Baltic Defence College.

Markus had been appointed as ambassador of the NATO Cooperative Cyber Defence Centre of Excellence where he had been course director and lecturer of various technical courses. For many years, he was track manager at CyCon, NATO's biggest conference on cyber defence, and he was program committee member as well as speaker at numerous international conferences in his fields of expertise. Markus has also been working as a cyber-security researcher for Fraunhofer FKIE's Cyber Analysis & Defense department for more than ten years focusing on resilience against novel cyber-attacks and on the development of trusted architectures. Based on this research, he is currently pursuing a PhD at the University of Bonn aiming to develop a framework for a future cyber arms control regime.

Syndicate Moderators and Keynote Speakers:

Major Alexander Bagus (JIC - Fusion Analyst Russia)

Alexander Bagus is a German Air Force Officer working as a Fusion Analyst at the Joint Intelligence Centre. In his current position, he focusses on Russian military threats on the joint operational level. Therefore, all military domains and dimensions in regards to Russia are part of his daily business.

Alexander studied history from 2006 until 2010 at the University of Würzburg and received a Master degree in Early Modern and Modern History, while serving as a reserve officer in the meantime. Afterwards, he found his way into the military intelligence branch of the Bundeswehr, as an active officer. In his early years as an analyst, he gathered experience in the analysis of asymmetric warfare in such countries as Jemen, Afghanistan and Mali.

Jan-Christoph Buchholz (ZCSBw – Cyber Threat Analyst)

Jan-Christoph Buchholz is a Political Scientist working as a cyber-threat analyst at the Bundeswehr Cyber Security Operations Centre. Besides routine threat analysis, his special focus is attribution of threat actors and meta-analysis of threats focusing especially on motivation and political background.

Jan-Christoph earned a Diploma in Public Administration from the German Federal University for Applied Public Administration in Bruehl and he graduated with a M.A. in Political Science from the University of Hagen; in both his research as well as from his multiple years of work experience the main focus of Jan's interests are the tradecraft of intelligence analysis, the organization of multi-level systems, and the democratic development after the Arabic Spring. Besides his academic background, Jan-Christoph obtained numerous professional certificates such as GSEC, GCED, GCIH, and GCTI.

Dr. Bernd Esser (Gartner – Director, former CISO BWI)

Bernd Esser is a Senior Director with Gartner Consulting and heads the Security practice for the DACH and Benelux regions. He supports CxOs of large organizations with all aspects of security strategy and its implementation. Bernd has more than 15 years of experience in management consulting and more than 25 years in security and data protection. Prior to joining Gartner, Bernd was the CISO at BWI, a state-owned federal IT service provider for the German Armed Forces and federal ministries and bureaus. Earlier to that, he had been with Deutsche Telekom as Director of CERT & Cyber Defence.

In addition to his professional employments, Bernd has been a long-term member of the DAX30 CISO working group and head of the DAX30 CERT/SOC working group. He has been a board member of the Deutscher CERT Verbund and is a regular chairman and keynote speaker at security conferences. He supported NATO as mission expert in a project to establish military CERT capabilities in a NATO-allied nation states. Bernd holds a Ph.D. from the University of Bonn and is fluent in English and German.

Lieutenant Colonel Christoph Kuehn (ZCSBw – Branch Head Cyber Threat and Risk Analysis)

Christoph Kuehn wears an Air Force Uniform but has ever since his exam in computer science from the Bundeswehr University in Munich in 1992 dealt with hard- and software rather than with airplanes. He wrote software, supported studies, managed projects, led CIS support teams and taught programming, applications and operating systems at a military education facility.

Since 2003 he headed international CIS support teams at three different units supporting NATO for a total of 13 years, including a six-month assignment to ISAF in Kabul. He joined the Cyber Security Operations Centre of the Bundeswehr in Euskirchen in 2018.

Prof. Dr. Michael Meier (Fraunhofer FKIE – Head of Cyber Security Department)

Michael Meier is full professor for IT-Security in the computer science department at University of Bonn and head of the Cyber Security Department at Fraunhofer FKIE. His research interests include most aspects of applied computer security, with an emphasis on attack and malware analysis as well as detection.

From 1993 to 1998 Michael studied computer science and earned his PhD in 2006 for his work on Intrusion Detection at Brandenburg University of Technology Cottbus. From 2006 he worked as Senior Researcher with the Information Systems and Security working group of the Technical University Dortmund before he became Professor in Bonn in 2012. Michael is founder member and chair of the special interest group on Security – Intrusion Detection and Response (SIDAR) of the German Informatics Society and co-chairs the steering committee of the international conference on Detection of Intrusion & Malware and Vulnerability Assessment. He is also executive board member of the German Association for Data Protection and Data Security (GDD).

Robert Mueller (Fraunhofer FKIE – Reseacher Cyber Analysis & Defense)

Robert Mueller works as an IT security researcher for Fraunhofer‘s Institute for Communication, Information Processing and Ergonomics FKIE. He accomplished a master degrees in Computer Science as well as in Communication Science. In 2016, Robert started his scientific career at the University of Applied Sciences Bonn-Rhein-Sieg where his research focused on automatically analyzing opinions in Twitter data as well as in technology-related journalistic articles. Since 2019, Robert manages a project at Fraunhofer FKIE aiming to automatically extract Cyber Threat Intelligence from plain text resources. Beside that, he deals with the research fields Cyber Situational Pictures in military contexts, as well as Secure Software Development and how to integrate related measures into existing processes.

Daniel Plohmann (Fraunhofer FKIE – Reseacher Cyber Analysis & Defense)

Daniel Plohmann is an IT security researcher at Fraunhofer‘s Institute for Communication, Information Processing and Ergonomics FKIE. He received his diploma in computer science at the University of Bonn in 2009.

Since 2010, Daniel has been studying malware families and botnets at the University of Bonn. Relevant work includes the ENISA botnet study, the analysis of various P2P protocols (e. g. from Gameover Zeus) and comprehensive analyzes of Domain Generation Algorithms. His primary research field is reverse engineering with a focus on the automation of malware analysis. Within this field of expertise, Daniel regularly holds workshops and lectures.

Captain Patrik Waeldin (ZCSBw – Cyber Threat Analyst)

Patrik Waeldin is an army officer working as a cyber threat analyst at the Bundeswehr Cyber Security Operations Centre. In his current position, he focusses on the analysis of open source intelligence and contributes to the advancement of analysis products in his work scope. Before this assignment, Patrick was a software tester in the military domain where he gained first-hand experience about software flaws and vulnerabilities.

Patrik started his academic career as a research assistant at Fraunhofer ISE working on the development OT systems within the scope of industrial control systems for managing solar power systems. Having received his Bachelor degree as an Electric Engineering, he obtained a Master degree in Computer Aided Engineering from Bundeswehr University in 2014.

Colonel Gerd Weiss (ZCSBw – Department Head CSOCBw)

Gerd Weiss has a long career as officer in der German Bundeswehr, mainly in the realm of communications and IT. This includes positions in the ministry of defence, as battalion commander, in the USA and NATO operation KFOR. His last posts have been all in support of cyber defence. For the last years he lead the Bundeswehr Cyber Security Operations Centre within the ZCSBw. Gerd holds a diploma in computer science from Bundeswehr University Munich.