NEWSROOM: Towards Automating Cyber Situational Awareness Processes and Tools for Cyber Defence

Markus Wurzenberger, Stephan Krenn, Max Landauer, Florian Skopik
firstname.lastname@ait.ac.at
AIT Austrian Institute of Technology
Vienna, Austria

Cora Perner
cora-lisa.perner@airbus.com
Airbus
Taufkirchen, Germany

Jarno Lötjönen, Jani Päijänen
firstname.lastname@jamk.fi
Jamk University of Applied Sciences
Jyväskylä, Finland

Georgios Gardikis, Nikos Alabasis
ggar@space.gr,nalabasis@space.gr
Space Hellas S.A.
Athens, Greece

Liisa Sakerman
liisa.sakerman@cr14.ee
Sihtasutus CR14
Tallinn, Estonia

Kristiina Omri
kristiina.omri@cybexer.com
CybExer Technologies OÜ
Tallinn, Estonia

Ulrike Lechner, Corinna Schmitt
firstname.lastname@unibw.de
Universität der Bundeswehr München
Neubiberg, Germany

Juha Röning, Kimmo Halunen
firstname.lastname@oulu.fi
University of Oulu
Oulu, Finland

Vincent Thouvenot
vincent.thouvenot@thalesgroup.com
ThereSIS, Thales SIX GTS
Palaiseau, France

Martin Weise, Andreas Rauber
firstname.lastname@tuwien.ac.at
TU Wien
Vienna, Austria

Vasileios Gkioulos, Sokratis Katsikas
firstname.lastname@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Norway

Luigi Sabetta, Jacopo Bonato
firstname.lastname.ext@leonardo.com
LeonardoLabs (Leonardo spa)
Rome, Italy

Rocío Ortíz, Daniel Navarro
ropayan@indra.es,dnmartinez@indra.es
INDRA
Alcobendas, Spain

Nikolaos Stamatelatos, Ioannis Avdoulas
firstname.lastname@logstail.com
Logstail
Athens, Greece

Rudolf Mayer, Andreas Ekelhart
firstname.lastname@univie.ac.at
University of Vienna
Vienna, Austria

Ioannis Giannoulakis, Emmanouil Kafetzakis
giannoul@8bellsresearch.com
mkafetz@8bellsresearch.com
Eight Bells Ltd
Nicosia, Cyprus

Antonello Corsi
antonello.corsi@cy4gate.com
CY4GATE SpA
Rome, Italy

ABSTRACT

Cyber Situational Awareness (CSA) is an important element in both cyber security and cyber defence to inform processes and activities on strategic, tactical, and operational level. Furthermore, CSA enables informed decision making. The ongoing digitization and interconnection of previously unconnected components and sectors equally affects the civilian and military sector. In defence, this means that the cyber domain is both a separate military domain as well as a cross-domain and connecting element for the

ARES 2024, July 30–August 02, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07
https://doi.org/10.1145/3664476.3670914

other military domains comprising land, air, sea, and space. Therefore, CSA must support perception, comprehension, and projection of events in the cyber space for persons with different roles and expertise. This paper introduces NEWSROOM, a research initiative to improve technologies, methods, and processes specifically related to CSA in cyber defence. For this purpose, NEWSROOM aims to improve methods for attacker behavior classification, cyber threat intelligence (CTI) collection and interaction, secure information access and sharing, as well as human computer interfaces (HCI) and visualizations to provide persons with different roles and expertise with accurate and easy to comprehend mission- and situation-specific CSA. Eventually, NEWSROOM's core objective is to enable informed and fast decision-making in stressful situations of military operations. The paper outlines the concept of NEWSROOM and explains how its components can be applied in relevant application scenarios.

CCS CONCEPTS

• **Security and privacy** → Cryptography; Security services; *Intrusion/anomaly detection and malware mitigation*; *Systems security*; *Network security*; *Software and application security*; • **Applied computing** → **Military**; *Cyberwarfare*; • **Computing methodologies** → **Artificial intelligence**; **Machine learning**;

KEYWORDS

Cyber Situational Awareness, CSA, Cyber Defence, Cyber Information Warfare, Mission-specific information

ACM Reference Format:

Markus Wurzenberger, Stephan Krenn, Max Landauer, Florian Skopik, Cora Perner, Jarno Lötjönen, Jani Päijänen, Georgios Gardikis, Nikos Alabasis, Liisa Sakerman, Kristiina Omri, Ulrike Lechner, Corinna Schmitt, Juha Röning, Kimmo Halunen, Vincent Thouvenot, Martin Weise, Andreas Rauber, Vasileios Gkioulos, Sokratis Katsikas, Luigi Sabetta, Jacopo Bonato, Rocío Ortíz, Daniel Navarro, Nikolaos Stamatelatos, Ioannis Avdoulas, Rudolf Mayer, Andreas Ekelhart, Ioannis Giannoulakis, Emmanouil Kafetzakis, and Antonello Corsi. 2024. NEWSROOM: Towards Automating Cyber Situational Awareness Processes and Tools for Cyber Defence. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30–August 02, 2024, Vienna, Austria.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3664476.3670914

1 INTRODUCTION

The emergence and ongoing interconnection of previously unconnected devices and components makes both civilian infrastructures, such as critical infrastructures, and military infrastructures vulnerable to cyber attacks. Specifically in case of critical and military infrastructures, reasons include legacy devices that are not designed for deployment in connected digital infrastructures as well as customized components, devices, and tools. Those components usually lack proper support from vendors and security providers, which leads to unpatched security vulnerabilities due to missing update support and absence of signatures for intrusion detection [15].

Furthermore, modern conflicts between nations and unions of countries are by no means limited to the physical world, i.e., battlefields and economic aspects, anymore. Rather than that, conflicts are increasingly dealt with in cyber space. Hence, modern conflicts are multidimensional and not restricted to certain areas and often involve a variety of sectors and methods [6, 12]. This is also referred to as hybrid warfare. Cyber attacks are often seen as a way to attack and harm a country without an official indication of hostile intentions, thereby bypassing organizations and committees such as the United Nations Security Council and mitigating expected consequences including economic sanctions [31]. This concept is also referred to as gray zone warfare [25]. Furthermore, this allows countries to outsource their criminal and hostile activities to third parties and groups such as advanced persistent threats (APT), which allows them to disguise their actions [41]. This leads to private adversarial groups equipped with high financial resources and advanced attack capabilities that carry out sophisticated malicious campaigns against civilian and military infrastructures in cyber space employing stealthy and hard to detect advanced and customized attack techniques. Their objectives range from influencing public opinions and elections to destabilize a country's governmental and societal structures, over disabling and destroying critical and military infrastructures, including health, energy, transport, and defence, to espionage, data theft, and stealing intellectual properties [2]. Given that these war-like activities also concern civilian and public cyber infrastructures, whose operators are often overwhelmed with such advanced attacks, cyber defence units are obliged to also protect these infrastructures alongside the military cyber environments [13].

Cyber Situational Awareness (CSA) is an important component in enabling cyber defence to deal with these multi-dimensional threats affecting various sectors that operate heterogeneous cyber infrastructures comprising a large variety of technologies with diverse cyber securtiy requirements. In general, the multifaceted topic of Situational Awareness (SA) splits into technical and cognitive aspects. The technical part of SA considers tools to compile, process and fuse data, thus focuses on relating and evaluating data and pieces of information relative to each other. On the other hand, the more actively researched cognitive part of SA covers the capacity to comprehend technical implications and draw conclusions that facilitate informed decision making. There exist three levels of SA that can be achieved [16]: (i) the perception of elements within a specified time frame, (ii) the comprehension of their meaning, and (iii) the projection of their status in the near future. CSA concerns the cyber space, which means it considers data from digital sensors, such as alerts from intrusion detection systems (IDS) and Cyber Threat Intelligence (CTI), such as reports from Open Sources Intelligence (OSINT) sources that are further processed and combined by other tools or directly interpreted by decision-makers. However, it is generally recommended not to consider the cyber space isolated from the real world. Therefore, information from cyber sensors are often combined with information from ordinary sensors, such as human intelligence reports, to enhance CSA overall. Taking a look at CSA from this point of view, perfectly matches the requirements of cyber defence as both a separate military domain and transversal layer of defence in general [10].

The need for advanced CSA technologies in the cyber defence community is known since several years [32]. Achieving a high-level of CSA in cyber defence and cyber security is a complex endeavour that touches and combines various technical areas and aligns many processes. The core objective of CSA in cyber defence is to provide all stakeholders, personnel of all levels in the chain

of command (e.g., in headquarters, in security operation centres (SOCs) on battlefields, or governmental organizations such as ministries of defence), and persons with different expertise that are active in different military domains accurate information about the current threat landscape and threat level. This is necessary to support establishing an appropriate cyber defence strategy and allow timely adaptation on tactical and operational level according to changes in the current operational picture and the evolving threat landscape. CSA in cyber defence must collect all available data from internal military network infrastructure (i.e., enterprise IT, servers, cloud infrastructure, etc.) and devices used by military units in operation and on battlefield (i.e., mobile user clients such as notebooks and tablets, Internet of military things (IoMT), etc.), which includes structured and unstructured data in the form of logs, sensor data, network traffic, internal intelligence (e.g., context information), and external information from both clear and dark net, such as CTI, vulnerability and malware reports, security bulletins, etc. However, the vast and continuously growing amounts of data and information challenge human operators to comprehend the overall threat picture. Therefore, CSA has to aim at automating and supporting several processes related to observing and analyzing these massive amounts of data and information. This includes recognizing attacks, classifying attacker behaviour, and supporting the process of filtering, correlating, and interpreting alerts. Additionally, CSA platforms have to present data and information to different users according to their specific needs, level of expertise, and current situation, for example, to personnel in battlefield and operation. Collaboration and information sharing between units, headquarters, among forces, with allied nations, and within the cyber defence community (e.g., SOCs, network operation centres (NOC), and computer emergency response teams (CERT)) meeting highest data integrity, sovereignty, and privacy standards of military level is important to obtain the most accurate information basis at all times. Finally, training military personnel in the application of CSA tools and procedures under highly realistic conditions is necessary to guarantee functioning CSA processes even under tense conditions in critical missions [24].

NEWSROOM takes a mainly technical approach and aims to meet these requirements and to address current challenges related to CSA, specifically in cyber defence. Therefore, NEWSROOM designs technologies and researches processes related to many aspects of CSA in cyber defence, including data and CTI collection, attacker behaviour and capability classification, human computer interaction (HCI) and visualizations, and information sharing. Furthermore, NEWSROOM aims to support decision-making on strategic, tactical, and operational level through accurate depiction of the current threat picture and detection of trends in the fast evolving threat landscape. Particularly, on tactical and operational level, NEWSROOM's designed technologies consider context information, such as mission specifications and asset databases, to filter most relevant information for the actors' current situation. In this context, an important objective of NEWSROOM is to provide CSA in an easily comprehensible way, taking into account the consumers' role and expertise to support accurate decsion-making in stress-full and tense situations. In this regard, this paper provides the following contributions to outline and introduce the NEWSROOM initiative [45]:

(1) A discussion of current challenges and pursued objectives related to CSA in the context of cyber defence, as well as how requirements, conditions, and scope are different to the civilian sector.
(2) A description of areas with potential of disruption that are addressed by NEWSROOM and which contributions the initiative aims to deliver.
(3) An outline of the NEWSROOM concept and how it integrates with the military domain and cyber defence community.
(4) A description of high-level scenarios and proposal how NEWSROOM technologies can contribute to improving CSA in the military domain.

The remainder of the paper structures as follows: Sect. 2 summarizes related work and Sect. 3 collects challenges related to CSA in cyber defence, requirements of cyber defence, and research objectives that should be addressed. Sect. 4 lists the areas NEWSROOM contributes to and Sect. 5 outlines NEWSROOM's concept. Finally, Sect. 6 describes scenarios and the applicaion of NEWSROOM before Sect. 7 concludes the paper.

2 RELATED WORK

As already mentioned in the introduction, CSA is a multilayered and complex topic. Franke et al. provided a general systematic literature review on this topic in 2014, reviewing more than 100 articles [10]. Today there exist several other surveys looking at specific aspects related to the topic, e.g., visualizations [20], or specific areas such as smart cities [33] or internet of things (IoT) [5]. Alavizadeh et al. provide an overview about all techniques, methods, and areas related to CSA. Their work demonstrates that there exist solutions and frameworks for single aspects of CSA such as data and information gathering and analysis, but there exist no integrated approaches or frameworks that connect the different technologies related to CSA [1]. Similarly, Husák et al. and Franke et al. discuss in their works challenges and issues related to CSA, and list all components and tasks relevant for CSA [9, 16]. Jajodia et. al present a framework that aims to integrate several CSA technologies [19]. CRUSOE is an approach that specifically focuses on the aspects of CSA that relates to decision support in incident handling [17]. Their work bases on the well-known OODA (Observe, Orient, Decide, Act) loop concept [48] and considers mission-centric elements, which relates their research to cyber defence and views CSA in a military context. The OODA loop is a concept that is also considered in the context of CSA in critical infrastructure protection [38].

Other works do not specifically focus on CSA technologies identified in state of the art literature. They take other approaches, such as increasing CSA in specific areas, such as Cyber Physical Systems (CPS), by employing digital twins to understand the current cyber situation [8]. Others focus on increasing CSA through training and exercises on cyber ranges and test-beds [44]. An important element of CSA that has been discussed in several articles is information sharing within communities [37], such as CERTs [21].

In the military domain, specifically the emergent and dynamic characteristics of cyberspace have led to an increased need of CSA [29]. A key requirement in this context is to present CSA in a mission-centric manner and to understand the interdependence

among mission elements, how mission elements depend on cyber assets, and how cyberattacks can potentially impact missions [14].

3 RESEARCH CHALLENGES RELATED TO CSA

Besides the multitude of technical and scientific challenges related to CSA [16], there are significant differences between the defence and civilian sector that need to be taken into account. The need for advanced CSA technologies in cyber defence is well-known since years [32]. The remaining section first discusses fundamental requirements and conditions that distinguish cyber defence from cyber security. Hereafter, the section formulates essential objectives that should be targeted when researching CSA in the context of cyber defence [11].

3.1 Cyber defence requirements to CSA

CSA for evolving computing environments is of key importance for both cyber defence, i.e., the military sector (cyber defence), and the civilian sector (cyber security). Therefore, there exist a certain overlap in the requirements and goals of these two domains. Consequently, there exist several technologies that both domains apply, for example, tools to collect data and information, classify attacker behaviour, share and visualize information, and access information via HCIs. This is also known as dual use and there exists potential to transfer available technologies and research between the two sectors. However, use cases, application scenarios, and requirements differ significantly, and tools need to meet military standards, such as a high level of information security. In particular, this concerns assets and values to protect, available resources, and data and information.

3.1.1 Assets and values to protect. In the private sector organizations only need to protect their own network infrastructure, which limits the scope significantly for most companies. In comparison, cyber defence needs to protect military, governmental, and critical infrastructures. Additionally, they need to defend a society's social and societal values against adversaries that attempt to influence the political system and bring a nation's governmental and critical infrastructure to a collapse. Therefore, cyber defence needs to monitor governmental and military systems and network infrastructure, as well as public networks, including clear and dark web (e.g., social media) to build CSA and observe the current threat landscape [43, 46].

3.1.2 Available resources. Private organizations invest only enough financial and human resources into cyber security as long as it optimizes their return on investment (RoI), using risk management methods such as game theory [27]. In cyber defence, the amount of needed human and financial resources to protect assets and values plays a subordinate role, since the value of a functioning state and society, and working critical infrastructures, such as electricity, supply chains, water supply, transport, and health, can hardly be expressed in numbers. However, the available personnel and budget for cyber defence are still limited. Therefore, cyber defence demands methods and algorithms for creating CSA that support military analysts in operation and mission most efficiently and reduce the required resources by automating processes such as attacker classification (e.g., aggregation, correlation, contextualization, attribution, and interpretation of alerts triggered by Intrusion Detection Systems (IDS)), filtering information and visualizing it with respect to a user's situation and demand in a mission-dependent way to aid comprehending vast amounts of data and information efficiently. These approaches also need to allow the use of less experienced personnel. Enabling trustworthy information sharing with allied partners and communities such as military CERTs, NOCs, and SOCs, supports collaboratively increasing CSA while simultaneously guaranteeing data privacy, sovereignty and integrity [18, 22].

3.1.3 Data and information. Private companies need to monitor data only in their own network infrastructure. CTI is mostly consumed by security providers and private SOCs. The private sector is mostly concerned with data privacy and IPR protection. Cyber defence must protect huge and diverse network infrastructures used by military, government, and critical infrastructures. These networks include legacy systems, cloud infrastructure, enterprise IT, and assets such as IoMT (e.g., drones), which makes data collection, storing, managing, and analysis for attacker classification a complex and labour-intensive task. Data sources are diverse and can occur in a dynamic and ad hoc manner depending on the cyber defence scenarios. Thus, CSA technologies that make use of artificial intelligence (AI) and machine learning (ML) to support human operators are necessary. Additionally, to supply cyber defence strategies and tactical postures with accurate and up-to-date CSA, information monitoring of CTI sources occurring in clear and dark web is vital to be informed about changes in the threat landscape and be able to react to emerging threats timely. To handle the seemingly infinite amount of information, AI and natural language processing (NLP) algorithms are needed that correlate, filter, rank, and rate information automatically to aid human operators and decision-makers in gaining CSA and taking accurate decisions. In opposite to the private sector, cyber defence also has to handle classified information, which increases the requirements for information security, confidentiality, and privacy. Hierarchical command structures and collaboration with allied partners and communities (e.g., SOCs, NOCs, and CERTs) requires rigorous access control to manage different classification levels. Finally, distributed ledger technologies (DLT) and cryptography tools are needed to guarantee information integrity and sovereignty [30].

3.2 Pursued objectives related to CSA

The complex nature of CSA complicates defining an exhaustive list of objectives. Taking into account the specific requirements of cyber defence, NEWSROOM identified the following ten areas as relevant objectives of CSA that related research should address:

(1) Identifying realistic application scenarios for CSA technologies in cyber defence missions;
(2) Deriving functional, non-functional, security, and interoperability requirements and designing an architecture for integrated CSA platforms;
(3) Studying available CTI and raw data sources to depict the current threat landscape and enable attacker behaviour classification;
(4) Researching and designing frameworks for federated learning (FL) and collaborative intrusion detection systems (CIDS);

(5) Employing digital twins to simulate IoMT and observing adversarial behaviour using deception technologies;
(6) Studying anomaly detection and alert aggregation methods to detect advanced attackers such as APTs and automate attack pattern mining;
(7) Applying NLP and AI to link CTI to alerts and attack patterns and enable automated attack interpretation;
(8) Designing HCIs and visualizations that provide mission-specific CSA information to military units;
(9) Assess information sharing methods to enable trustworthy collaboration among allied countries to increase CSA;
(10) Develop cyber range environments and scenarios for training military personnel in CSA processes and use of CSA technologies.

In this context, NEWSROOM pursues five research objectives.

3.2.1 Design application scenarios for CSA in cyber defence. The design of relevant and realistic application scenarios related to the domain of cyber defence is essential to guarantee future acceptance and applicability of research results. these scenarios build the foundation for requirements elicitation, which informs state of the art analysis to derive open research gaps [47].

3.2.2 Improve data insights. This objective relates to collecting and aggregating raw data, e.g., logs from systems, sensors, and IoMT and OT components, as well as network traffic. This includes also crawling clear and dark Web for CTI [23]. Considering frameworks that enable the implementation of concepts such as federated learning (FL) [39], transfer learning (TL) [7], and collaborative intrusion detection systems (CIDS) [28] allow to improve efficiency of training detection algorithms that implement machine and deep learning, and improve detection accuracy through combining various detection algorithms [3].

3.2.3 Establish actionable CTI to improve attacker classification. Aggregating and correlating heterogeneous alerts from various IDSs enables automatic attack pattern mining. These attack patterns supply the CSA picture. Linking them to CTI, such as currently observed attackers tactics, techniques and procedures (TTP) is a first step to automating attack interpretation. Furthermore, sharing created attack patterns with other stakeholders operating similar cyber infrastructures, elevates them to actionable CTI [26, 30].

3.2.4 Develop advanced HCI and increase integrity and privacy of information sharing to support collaborative CSA. It is important to visualize information in an advanced way taking into account person's roles, experterise, and mission-specific requirements to support military staff in capturing the current operational picture and threat landscape. Sophisticated HCIs need to enable smooth interaction with CSA information. To facilitate acceptance of sharing information and thus encourage the desire to collaborate among different military domains, within the entire national cyber defence, and allied nations, it is of utmost importance to enhance trust in data and information sharing. This includes, adopting advanced encryption technologies and approaches that allow implementation of the need-to-know-principle to reduce risk of data and information leaks. Eventually, to raise acceptance for smart CSA technologies by personnel of all levels in the chain of command ranging from military units at operational level to persons in MoDs at strategic level, advantages closely associated with the military domain, such as assisting the processes of building CSA pictures that meet the requirements to address the fast evolving threat landscape and providing mission-oriented information tailored to the current situation, mission, and needs of a unit, must be emphasized [20, 36, 42].

3.2.5 Design future-proof CSA platform architectures and define efficient collaborative processes. Following modular design principles, when designing integrated CSA platform architectures, ensures easy adaptability and extentions with new technologies to comply with requirements emerging in the future. The heterogeneous nature of the military sector, splitting into different domains (land, air, sea, space, and cyber) and the even greater scope of military operations, including critical, public, and governmental infrastructures, leads to a vast amount of varying demands to CSA processes and technologies. Hence, various processes and guidelines must be aligned to establish a CSA framework that enables collaboration across military domains. Therefore, benefits of such integrated CSA solutions must be communicated to the different stakeholders at an early stage in an easily comprehensible manner. Continuous integration of end users during all phases of design and development is required to ensure future acceptance of research results [1].

4 POTENTIAL OF DISRUPTION IN CSA

Achieving the objectives related to CSA identified in Sect. 3.2 requires significant advancements beyond the state of the art in several areas of cyber defence and security. Therefore, NEWSROOM aims to contribute to nine areas with potential of disruption (PoD).

PoD1: CTI and data collection for CSA: Collected data and CTI build the foundation for all other CSA processes and tasks. To achieve a complete CSA picture, raw data from various sources, such as system, network, and sensor logs, network traffic, and clear and dark Web CTI, needs to be collected and normalized. Reasons are that different attack steps manifest in different data sources and that CTI can be content of any unstructured free text such as a forum entry, mailing list post, security bulletin, threat or vulnerability report, or social media post, among many others. Eventually, to enable further analysis on a complete data and information base, all these sources have to be converted into a common format or be accessible from a single location. Specific challenges in this area are methods for normalization and crawling of CTI.

PoD2: Collaborative and federated learning: Since training advanced AI and deep learning (DL) algorithms has challenging requirements regarding computational resources and the available training data, there is a demand for frameworks implementing collaborative, federated, and transfer learning. Major research challenges in this area are (i) guaranteeing private, secure, and decentralized algorithms for local but collaborative training, (ii) prevention from attacks, such as poisoning and adversarial AI against collaborative training environments, and prohibition of data and AI model leakage, and (iii) overcoming challenges towards the development of CIDS caused by the heterogeneous nature of infrastructures cyber defence has to deal with.

PoD3: Deception tools and digital twins: Deception tools such as honeypots, honeytraps, and decoys provide an environment that

enables observing actual attacker behavior, and thus analyzing currently used attack techniques without endangering any military and critical infrastructures. Because of the emergence of IoMT and increased interconnection of military devices, the simulation of realistic infrastructure requires the development of digital twins enriching infrastructures used by deception technologies with best possible realism attracting advanced attackers such as APTs. Finally, digital twins of IoMT are an essential playground to study future attack vectors against these network components and reveal vulnerabilities before adversaries can exploit them.

PoD4: Attack behavior classification: Signature- and rule-based detection perform well in classifying known attack behavior in conventional IT infrastructures. However, military and critical infrastructures connect a large variety of systems and components such as cyber physical systems (CPS), IoT, IoMT, and operational technologies (OT), as well as legacy systems, customized systems and systems with small market share, which lack signatures to classify attacks. Furthermore, military and critical infrastructures are predominantly targeted by advanced adversaries such as APTs, who employ sophisticated stealthy attack techniques that often exploit zero-day vulnerabilities and use customized malware, which are specifically hard to detect. Thus, anomaly detection methods, that build upon AI, ML, and DL require further improvement. Currently those approaches suffer from alert flooding, due to large numbers of false alerts and duplicated alerts, which leads to cumbersome post-processing by human analysts. Promising solutions to that are, for example, alert aggregation algorithms that automate attack pattern mining, and support filtering of duplicated and false alerts, and thus support human analysts in their triage. Furthermore, generated attack patterns are actionable CTI that can be shared within a community operating similar cyber infrastructures and attack behavior classification. Finally, attack behavior classification demands researching AI that automates linking detected alerts and attack patterns with CTI to support attack interpretation.

PoD5: HCIs and visualizations: HCIs and visualizations are the core elements of CSA technology stacks that depict CSA pictures and enable human operators to interact with the current situation picture and available CSA information. Therefore, these are the components that are most closely related to the cognitive aspects of CSA. They need to support perception, comprehension, and projection on all levels of the chain of command, which, for example, requires visualizations that are easy to comprehend, even during stressful situations. Furthermore, to serve the complex environment of cyber defence, it is necessary to develop solutions that take into account mission specific circumstances, and employ, for example, mission-models to provide CSA tailored to current operations to enable military personnel with different expertise and roles to take informed decisions fast even under tense conditions. Therefore, solutions that remove distracting elements that both disguise important insights or include excessive details beyond the expertise of personnel outside of, for example, SOCs. Promising tools to achieve these ambitions are large language models (LLM) and NLP algorithms.

PoD6: Expand trust boundaries for CTI sharing: Sharing CTI enables collectively improving cyber defence and cyber security against continuously evolving and newly emerging threats targeting increasingly complex and interconnected military and critical infrastructures. Additionally, sharing CTI with allied nations and within unions of allied nations can have a tremendous impact on improving a country's cyber defence. Allied countries often operate similar infrastructures and components, such as IoMT and battle systems, e.g., unmanned aerial vehicle (UAV), and are thus often vulnerable to the same threats and targets of the same hostile actors. Hence, immediately sharing CTI about current cyber incidents and attacks allows allied nations to timely adapt their cyber defence tactics and operations to defend their assets against emerging threats. Therefore, research of modern encryption methods, such as attribute-based encryption (ABE) is necessary to be ready for post-compromise security. Furthermore, DLT and procedures to enforce the need-to-know principle ensure information integrity and confidentially, and thus can increase trust in sharing CTI.

PoD7: CSA platform design: Because of the large diversity of technologies contributing to CSA and their disruptive character, it is important to research designs of future-proof architectures for CSA platforms that allow for modularity and thus enable extension as soon as new CSA technologies emerge. The involvement of a large variety of stakeholders and persons with heterogeneous expertise in the field of cyber defence require the design of processes and guidelines that meet their multi-dimensional requirements. Resulting architectures and processes are elements that guide the implementation of integrated CSA platforms.

PoD8: Scenarios and requirements: To put research related to CSA on a solid foundation and ensure future adoption by cyber defence stakeholders, the definition of realistic and relevant application scenarios in close collaboration with end-users and stakeholders is necessary. This includes the design of scenarios that scope situations, threat level, and conflict stages, formulation of storylines that describe concrete attack cases and specific interactions related to the scenarios, the structured preparation of vignettes that include technical details of storylines and eventually enable the specification of concrete use cases that allow for researching, evaluating, and testing of CSA technologies. Furthermore, these provide a foundation to design training and exercises related to the application of CSA tools and processes. Additionally, scenarios, storylines, and vignettes meeting military standards and needs are the starting point for requirements elicitation. Requirements inform state of the art analysis, which reveals research gaps to be filled.

PoD9: Cyber ranges for training and mission: Cyber ranges enable the simulation of scenarios, storylines, vignettes, and use cases and therefore provide realistic conditions for evaluating, testing, and training with CSA technologies. However, to increase realism of cyber ranges, they require integration of digital twins and emulations of IoMT and other OT. Designing cyber range environments that enable simulation of realistic networks replicating military and critical infrastructures is thus significantly harder than simulating conventional enterprise IT networks. The same virtualization and simulations used for cyber ranges can contribute to deception technologies mentioned previously.

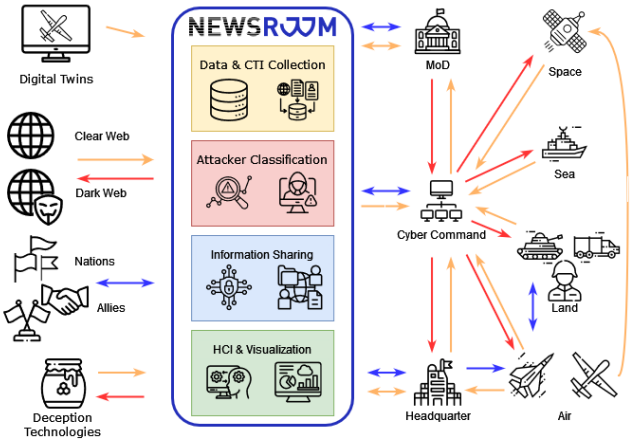

Figure 1: NEWSROOM concept: The color of the arrows relate to the components of NEWSROOM and exemplary show how different entities could use NEWSROOM. Green arrows are omitted since HCI and visualizations affect all users.

5 NEWSROOM CONCEPT

NEWSROOM pursues all objectives listed in Sect. 3.2 and will contribute to the state of the art as described in Sect. 4. The remaining section outlines the resulting concept of NEWSROOM and its application. Figure 1 depicts the concept and supports the description.

The core of NEWSROOM combines and integrates all dimensions of CSA. Thus NEWSROOM studies and designs concepts, methods, algorithms, frameworks, and guidelines with respect to cyber defence and in military context. Figure 1 shows that NEWSROOM's four main pillars consist of (i) collecting data and CTI, (ii) classifying attacker behaviour, (iii) information sharing, and (iv) visualizing information and providing human computer interfaces (HCI). Therefore, NEWSROOM covers all essential components of CSA previously described. These components are essential for gathering information, such as CTI to understand the current threat landscape and to generate contextualized CSA pictures and for collecting raw data to enable intrusion detection with innovative anomaly detection algorithms. Developed algorithms are combined in frameworks for FL, TL, and CIDS to provide a current operational and situational picture related to attackers in the cyber space. NEWSROOM employs alert aggregation to correlate alerts and automatically generate attack patterns that are robust against poisoning as well as adversarial artificial intelligence and machine learning (AI/ML) and support military personnel in prioritizing security events to react timely to emerging threats. NLP and AI algorithms support connecting alerts and attack patterns with CTI, including available information on exploits, vulnerabilities, IoCs, TTPs, and potential mitigation actions. By linking low level alerts with high level CTI and context information, NEWSROOM automates the process of interpreting attack traces, and connecting attacks to threat actors, such as APTs, and hostile countries. Additionally, it enables frequent updates of the current threat landscape and accurately depicting the current situation picture.

Particularly, to adapt cyber defence strategies, tactics, and operation timely to new attack vectors and threats, collaboration and sharing information with allied nations is important. Therefore, NEWSROOM assesses and designs DLT, cryptography concepts, and access control mechanisms to ensure data integrity and sovereignty, and to protect information against theft from hostile countries, which may support adversaries in evading cyber defence mechanisms. Cyber defence operation and mission requires collaboration of many different levels of the chain of command, ranging from deployed units, to headquarters, and governmental institutions. Therefore, NEWSROOM studies and designs methods for visualizing and supplying information to provide both (i) an overall CSA picture across multiple units and domains (e.g., for headquarters and high-level commands), as well as (ii) targeted mission-specific information to support personnel in tense situations as efficiently as possible. Beyond that, NEWSROOM focuses on cyber defence for modern digital and connected military assets, including IOMTs, such as UAVs. For this purpose, NEWSROOM designs digital twins to analyze threats and attacks against IoMT and supports training in relevant scenarios. Deception technologies, such as honeytraps, honeypots, and decoys allow NEWSROOM to observe and analyze actual adversarial behaviour without exposing and endangering military network infrastructures and sensitive information. Finally, NEWSROOM engages with stakeholders and end-users to design realistic application scenarios that allow to evaluate CSA components. The scenarios will be deployed in cyber ranges to demonstrate a mission-specific application of NEWSROOM's results and provide an environment for training military personnel in CSA processes.

An integral part of NEWSROOM is to provide a platform for collaborative CSA to connect the entire military chain of command, governmental institutions and authorities, national cyber defence communities, and allied countries. In this context NEWSROOM connects units in operation, headquarters, cyber defence units and infrastructure, and builds a link across different military domains (land, air, sea, space, and cyber) and to allied partners and communities. The application scenarios in the next section further elaborate on these elements.

6 APPLICATION SCENARIOS

In military context and cyber defence, mission engineering, as well as scenario development for simulation, exercise, and training, distinguish between the concepts scenario, storyline or vignette, and use case. Considering this framework, scenarios provide the scope of a hypothetical or fictional situation or sequence of events, i.e., a background story that sketches the historical, political, military, economic, cultural, humanitarian and legal events and circumstances of the conflict or crisis at hand. This includes descriptions of affected areas, e.g., countries, maps, plans, main actors, strategic situations, such as conflict, combat stages, or related crises. A storyline or vignette outlines one specific developing situation or sequence of events within a broader context, e.g., a scenario, which in context of cyber defence could be the detailed description of the sequence of events related to a single multi-step attack by an APT, including a clear description of the steps in the cyber kill chain, adversaries TTPs, and the defenders options to respond. NEWSROOM considers a storyline as a descriptive and less technical documentation of a sequence of events within a scenario and a vignette as the technical

expression of a storyline. Eventually, a use case is a description of specific tasks or interactions, such as "Actor A applies tool T to achieve X" [34, 35, 40].

The remaining section outlines the four scenarios NEWSROOM will employ to guide its research, evaluation of project results, and training and exercises in the context of CSA. Finally, the section will provide a specific example for a storyline and elements of vignettes.

6.1 NEWSROOM scenarios

NEWSROOM identified four scenarios that describe different stages of a conflict, crisis, and defence. They consider four different threat levels: (i) no threat, (ii) low threat-level, (iii) increased threat-level, and (iv) high threat-level.

6.1.1 Capacity building: CSA training and mission. At all times, even if there are no threats on the horizon, it is necessary to train and exercise personnel and prepare military staff of all units for future defence missions. CSA is an important part of an efficient and complete cyber defence strategy. It builds the backbone for developing strategies and tactics to defend future threats in cyber space that may affect all military domains and command levels, because today's communication and coordination, as well as operation heavily relies on cyber infrastructures. Thus, it is indispensable to properly train military personnel to build capacities in CSA to be able to accurately interpret the current threat landscape and build a complete Common Cyber Operational Picture (CCOP). Additionally, it is important to acquire capacities and analytical skills to use available CSA sources, including CTI and attack behaviour classification algorithms, to timely predict future threat scenarios.

In this regard, NEWSROOM develops relevant and realistic storylines and vignettes that take into account strategic and tactical aspects both technical and non-technical to provide a foundation for capacity building. By identifying common operational principles (CONOPS), and functional, security, and interoperability requirements, NEWSROOM provides guidelines on applying integrated CSA platforms for cyber defence, on governing cooperation among military forces and allied countries, and on establishing tactical postures. To enable realistic training and exercise conditions, NEWSROOM develops cyber range environments that simulate both digital infrastructure and physical infrastructure across domains, through the integration of IoMT, using emulation and digital twins, for example, of UAVs. Therefore, NEWSROOM enables training application of CSA technologies and strategic procedures such as collaboration between different forces and countries.

6.1.2 Isolated cyber attack against a single country. Monitoring of critical infrastructures and military infrastructures, as well as network activities and communication in public and social networks, are the main activities related to CSA in cyber defence context during low threat levels and outside of active conflicts. During such threat situations, predominantly isolated attacks against a single target and country are expected, especially if there is no evidence for planned adversarial campaigns in any information stream (e.g., social media, clear and dark web). Such isolated attacks, for example, aim at single targets of critical infrastructure, such as a single power plant or substation, or a single public authority/agency (e.g., data theft attempts or DoS). These attacks raise alerts in IDS that need to be analysed by cyber defence experts to trigger proper mitigation actions, revise preventive tools, such as rule-based attack detection and prevention mechanisms as well as reviewing and updating configurations of passive detection tools (e.g., anomaly detection), document the incident, and inform allied partners.

To accomplish these tasks, NEWSROOM provides solutions to collect and analyze low-level data such as system logs, sensor data, and network traffic for attack detection and classification. Furthermore, NEWSROOM crawls CTI to interpret alerts, recognize emerging threats, and identify changes in the threat landscape. Automating this processes and using, for example, unsupervised attack pattern mining, improves the efficiency and accuracy of attacker behaviour classification. Thus, cyber defence personnel can react faster and reliably against emerging threats and limit damage through early containment and triggering of mitigation actions. Combining attacker classification and information sharing allows to create actionable CTI, such as attack patterns that connect IoCs to information about threat actors (countries, IPs, type of attacker). Hence, NEWSROOM increases CSA for cyber defence and provides the tools for generating CTI data bases, such as an APT catalogue that correlates information about threat actors, their preferred TTPs, and country of operation to support the process of implementing efficient cyber defence strategies that address the current threat landscape. NEWSROOM's modular design enables coordination across all military domains, headquarters, with national authorities/agencies (e.g., SOCs, NOCs and CERTs), and with allied countries to stop spreading of cyber threats.

6.1.3 Operation during strategic defence. Strategic defence missions usually take place in times of increased threat level. Such situations occur, for example, if there is adversarial aggression close to borders of allied countries, or when there is a war fought close to allied countries borders. Under such circumstances, allied troops are on increased alert. There are increased reconnaissance missions of all domains and an elevated volume of communication and coordination between allied countries. In such defence scenarios CSA has to accomplish three fundamental tasks: (i) Monitoring of network infrastructure for communication, coordination and operation between headquarters and deployed units, including assets such as IoMT, (ii) continuously updating the current CSA picture and informing about the current threat landscape in cyber space, since large attack campaigns by advanced threat actors such as APTs and state-supported actors of hostile countries can take place at any time, and (iii) sharing relevant threat information with different units, i.e., providing targeted information adapted to the current situation of each unit and technology in use, and communicating novel CTI with allied partners.

NEWSROOM's proposal of a modular and future-proof architecture for integrated CSA platforms aims to simplify collaboration among allied nations that might use different technologies. Furthermore, NEWSROOM's approach to enforce the application of the need-to-know principle and to use post-compromise cryptography technologies increases trust and promotes sharing information among different units within a country and with allied nations. The use of deception technologies emulating realistic military and critical infrastructures leveraging the concept of digital twins for IoMT, OT, and other CPS, attracts actual attackers, which allows studying

adversarial behavior and TTPs in separated environments under secure conditions. Furthermore, these environments can serve as playground to identify vulnerabilities in network components and thus enable closing them before adversaries can exploit them. Versatile visualizations and HCIs enable personnel with different roles and expertise to efficiently interact and consume CSA information even in tense and stressful situations. Thus, NEWSROOM supports taking informed decisions on all levels in the chain of command.

6.1.4 Large-scale coordinated attack against specific sectors and several allied nations. Military domains and other infrastructures are increasingly intertwined with activities in cyberspace. Since modern cyber defence operations rely on digital infrastructures for communication and coordination, both headquarters and deployed units are vulnerable to cyber threats. While the previous scenario covers CSA tasks related to military infrastructure, this one focuses on cyber defence of countries, assets, critical infrastructure, and societal values in general. Today, countries are connected digitally and physically share critical infrastructures, for example, transport infrastructures and power grids. Hence, critical infrastructures are a relevant target for threat actors such as hostile nations, APTs, and cyber terrorists that threaten allied countries on a large scale with coordinated attacks and cause significant damage that affects safety of citizens, economy, and social life. In the past, notable attacks on power grid infrastructure have been documented, such as in the Ukraine [4]. A successful attack on critical infrastructure, such as the power grid, would propagate unpredictable negative effects far beyond the energy sector deep into a community's economy and society. Moreover, such a scenario may include an evolving series of single attacks, cascading effects leading to dynamic situation that requires collaboration between military and non-military actors. To successfully defend such attacks and limit the impact, it is indispensable to possess a CSA strategy and infrastructure that allows collaboration, coordination, and communication of tactical and operational activities across a country's military domains and with allied nations. To defend such attacks, CSA must provide up-to-date situation pictures of targeted sectors, a CSA picture that covers the current threat landscape for each sector individually and across related sectors, an operational picture that involves forces of several countries, and ensure trustworthy and reliable sharing of relevant CTI to enable accurate and timely cyber defence missions.

NEWSROOM deception technologies allow to obtain CSA about adversaries current TTPs. Advanced visualizations and HCIs aim to make CTI actionable for military staff in cyber defence, adjusted to different operation and mission situations. NEWSROOM's technologies to improve the conditions for information sharing described previously, support allied nations to collaboratively obtain complete CSA pictures and compile specifications of the current threat landscape across countries.

6.2 NEWSROOM application

The remaining section describes an exemplary storyline and vignettes related predominantly to a situation of low threat-level as outlined by the scenario described in Sect. 6.1.2. Furthermore this section elaborates on the application of NEWSROOM in course of the sequence of events.

The storyline at hand considers a situation that involves UAVs observing a countries border next to a hostile country. UAVs are an example for modern and complex IoMT devices in military infrastructures. Figure 2 provides an overview of the involved components and network infrastructure. This storyline involves the military domains cyber, air, and space. Two UAVs, A and B, are controlled from a headquarter using a military command and control (C2) infrastructure that primarily communicates via satellite and offers radio and cellular as alternative communication channels. The UAVs include a battlefield management system and communicate with each other over a mesh WiFi network. During the observation mission for a brief period of time, UAV A enters the neighbouring country's airspace. The hostile country has been awaiting a long time such a situation that allows them to attack an UAV under justified conditions. There are several tactical vignettes with different causes that can be described here. Examples for vignettes from the adversaries point of view are (i) an attack that compromises the C2 infrastructure in the headquarter to manipulate the UAV operation, (ii) a supply chain attack where a malware on an UAV has been deployed by an insider, (iii) jamming the communication to force the UAV to land, or (iv) attacking the mesh WiFi between the UAVs to gain access to the C2 infrastructure via cellular communication. Objectives of the adversary include stealing an UAV to collect intelligence on the technology, infiltrating the military network infrastructure, and financial damage.

The storyline and the described vignettes of the adversary allow for the application of all NEWSROOM components. First, we assume that the NEWSROOM platform collects data from all involved systems and components, including logs, network traffic, and sensor data. Furthermore, it continuously crawls CTI from clear and dark Web and gathers CTI through information sharing with allies and communities the country is partner in. Already before mission operation, NEWSROOM has a significant impact on the mission. First, digital twins of the UAVs have been used to test the UAVs and attack detection against attacks suggested by the current threat picture provided by NEWSROOM. Therefore, potential incidents have already been known or counter measures could have been taken that eliminated certain threats. Additionally, the digital twin has been used in deception technologies. Therefore, a potential outcome of the vignettes could have been that the adversary ends up in a honeytrap and the defending country is able to observe his TTPs under secure conditions in a separated system and take measures against them. CTI collected during this activity could be shared with allied nations that operate similar UAV infrastructures. Therefore, the countries community would have been save from the studied attacks and could securely observe their boards using the UAVs. In this situation also attacker classification could have been trained based on the data collected with the deception technologies. Finally, the unit operating the UAVs has defined mission models including information about the assets, i.e., the IoMTs, e.g., the UAV, the area they will observe, the communication channels they use, and the C2 system. These mission models later will enable NEWSROOM to provide all involved personnel with mission-specific CTI and thus enable fast and accurate decision making.

Assuming that the attack could not be prohibited before the observation mission, the cyber defence unit that has been assigned the task to monitor the border observation mission is continuously

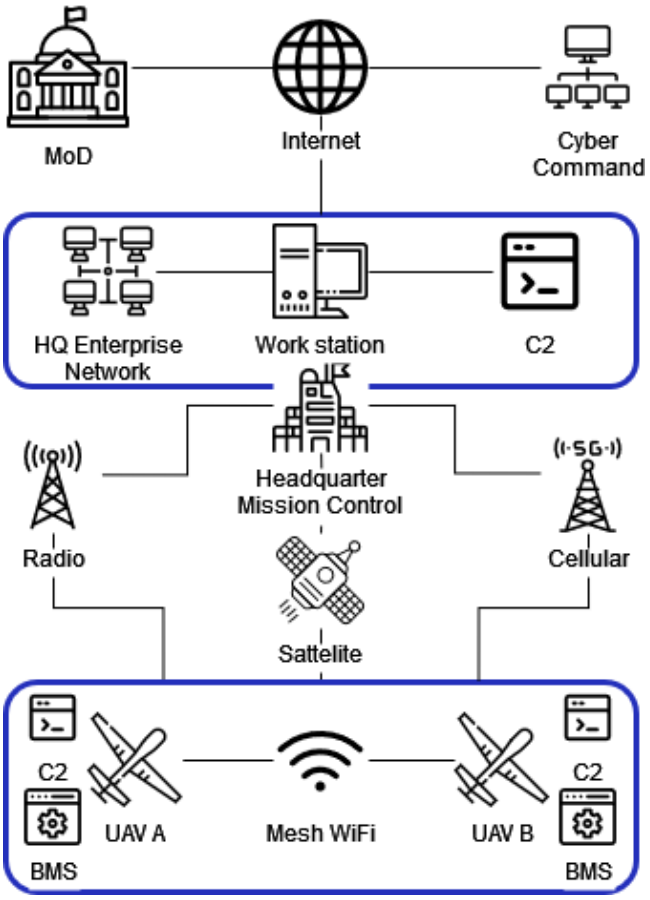

Figure 2: Infrastructure of a vignette considering UAVs.

provided with alerts and attack patterns from attacker classification. However, due to the previously defined mission models and increasing CTI reports related to the UAV models, alerts related to the UAVs are ranked higher. We assume the adversaries jam the communication of the UAV that entered the hostile airspace. This triggers an alert based on the altered communication between UAV A and UAV B via their mesh WiFi. Consequently, the cyber defence unit increases the monitoring verbosity for the involved infrastructure and shares information about the attack with personnel in charge of satellite communication and the UAV operation. Given the role and expertise of these units, NEWSROOM does not depict any technical details, merely provides information about affected devices and a predefined sequence of countermeasures. The unit operating the UAVs, for example, receives GPS coordinates of the attacked UAV and thus takes care that the other UAV is brought back deeper into the country's own airspace. On the other hand, NEWSROOM presents, based on the mission models, CTI related to the involved components to the cyber defence unit, which immediately starts mitigation actions and initiates forensic analysis. In case of an attack compromising the C2 infrastructure or a supply chain attack that enables the adversary to infiltrate the network infrastructure, CTI would be a source about expected next steps of the adversaries and online, i.e., live, and forensic attack classification would be important sources to inform the current situation picture. Finally, also the person (commander) in charge of the operation receives a report about the incident via NEWSROOM, provided with the option to share the information with allied nations. Since NEWSROOM implements the need-to-know principle, the platform proposes to share information about the attack with two groups, a higher ranked group of allied countries sharing a border with the adversary and operating the same or similar UAV infrastructure, and other allied countries operating the same or similar UAV infrastructure but not sharing a border with the adversary. The commander in chief decides to immediately share the information with the more important group and starts assessing if sharing with others is necessary as well. In the description, persons with different roles and expertise have been involved. During all steps the human military operator was in the loop. However, thanks to NEWSROOM, all activities could take place simultaneously, thus limiting the damage for the defending country and immediately protecting allied countries from the same attack, with significant potential for automation of these steps.

7 CONCLUSION

NEWSROOM is a research initiative to CSA specifically targeting technical aspects related to cyber defence and military applications. NEWSROOM designs methods, tools, and algorithms that relate to the topics data and CTI gathering, attack classification, secure and trusted information sharing, HCI, and visualization. Furthermore, NEWSROOM aims to deliver a modular and therefore future-proof architecture for integrated CSA platforms. A major concept NEWSROOM focuses on is to improve interaction with CSA depending on the role and expertise of a person to enable informed decision making on all levels of the chain of command even in tense and stressful situations. A cornerstone in this regard is providing CSA information and situational pictures that relate to current missions and situations of personnel. Thus, NEWSROOM contributes to all three levels of CSA: perception, comprehension, and projection.

In this paper, we discussed the objectives of NEWSROOM, the areas NEWSROOM contributes to, and the general concept of NEWSROOM. Furthermore, we compared military (cyber defence) to civilian (cyber security) requirements. Finally, we introduced application scenarios and an exemplary story line and vignettes that concern UAVs. In this regard, we outlined the application of NEWSROOM and how it affects different stakeholders and end-users.

ACKNOWLEDGMENTS

Funded by the European Union under the European Defence Fund (GA no. 101121403 - NEWSROOM). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

[1] Hooman Alavizadeh, Julian Jang-Jaccard, Simon Yusuf Enoch, Harith Al-Sahaf, Ian Welch, Seyit A Camtepe, and Dan Dongseong Kim. 2022. A survey on cyber situation-awareness systems: Framework, techniques, and insights. *Comput. Surveys* 55, 5 (2022).

[2] Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. 2019. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials* 21, 2 (2019).

[3] Iram Arshad, Saeed Hamood Alsamhi, Yuansong Qiao, Brian Lee, and Yuhang Ye. 2023. A novel framework for smart cyber defence: a deep-dive into deep learning attacks and defences. *IEEE Access* (2023).

[4] Defense Use Case. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* 388, 1-29 (2016).

[5] Angelo Corallo, Mariangela Lazoi, Marianna Lezzi, and Angela Luperto. 2022. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry* 137 (2022).

[6] Fabio Cristiano and Bibi van den Berg. 2023. Hybridity and Conflict in Cyberspace. *Hybridity, Conflict, and the Global Politics of Cybersecurity* (2023).

[7] Islam Debicha, Richard Bauwens, Thibault Debatty, Jean-Michel Dricot, Tayeb Kenaza, and Wim Mees. 2023. TAD: Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems. *Future Generation Computer Systems* 138 (2023).

[8] Matthias Eckhart, Andreas Ekelhart, and Edgar Weippl. 2019. Enhancing cyber situational awareness for cyber-physical systems through digital twins. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE.

[9] Ulrik Franke, Annika Andreasson, Henrik Artman, Joel Brynielsson, Stefan Varga, and Niklas Vilhelm. 2022. Cyber situational awareness issues and challenges. In *Cybersecurity and Cognitive Science*. Elsevier.

[10] Ulrik Franke and Joel Brynielsson. 2014. Cyber situational awareness–a systematic review of the literature. *Computers & security* 46 (2014).

[11] Darko Galinec, Darko Možnik, and Boris Guberina. 2017. Cybersecurity and cyber defence: national level strategic approach. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije* 58, 3 (2017).

[12] Carlos Pedro Gonçalves. 2019. Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats. In *Cyberspace*. IntechOpen.

[13] Global Governance. 2001. The internet and the changing face of international relations and security. *Information & Security* 7 (2001).

[14] William Heinbockel, Steven Noel, and James Curbo. 2016. Mission dependency modeling for cyber situational awareness. In *NATO IST-148 Symposium on Cyber Defence Situation Awareness*. NATO Sofia, Bulgaria.

[15] William Hurst and Nathan Shone. 2024. Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation. In *Management and Engineering of Critical Infrastructures*. Elsevier.

[16] Martin Husák, Tomáš Jirsík, and Shanchieh Jay Yang. 2020. SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*.

[17] Martin Husák, Lukáš Sadlek, Stanislav Špaček, Martin Laštovička, Michal Javorník, and Jana Komárková. 2022. CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. *Computers & Security* 115 (2022).

[18] Yadigar N Imamverdiyev et al. 2015. CYBER-TROOPS: FUNCTIONS, WEAPONS AND HUMAN RESOURCES. *Problems of information society* (2015).

[19] Sushil Jajodia and Massimiliano Albanese. 2017. An integrated framework for cyber situation awareness. In *Theory and Models for Cyber Situation Awareness*. Springer.

[20] Liuyue Jiang, Asangi Jayatilaka, Mehwish Nasim, Marthie Grobler, Mansooreh Zahedi, and M Ali Babar. 2022. Systematic literature review on cyber situational awareness visualizations. *IEEE Access* 10 (2022).

[21] Marc-André Kaufhold, Jennifer Fromm, Thea Riebe, Milad Mirbabaie, Philipp Kuehn, Ali Sercan Basyurt, Markus Bayer, Marc Stöttinger, Kaan Eyilmez, Reinhard Möller, et al. 2021. CYWARN: Strategy and technology development for cross-platform cyber situational awareness and actor-specific cyber threat communication. (2021).

[22] Ilker Kilaz, Akif Onder, and Murat Yanik. 2014. Manpower Planning and Management in Cyber Defense. In *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece*.

[23] Paris Koloveas, Thanasis Chantzios, Christos Tryfonopoulos, and Spiros Skiadopoulos. 2019. A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence. In *2019 IEEE World Congress on Services (SERVICES)*, Vol. 2642. IEEE.

[24] Alexander Kott, Cliff Wang, and Robert F Erbacher. 2015. *Cyber defense and situational awareness*. Vol. 62. Springer.

[25] Armin Krishnan. 2022. Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict. *Journal of Strategic Security* 15, 4 (2022).

[26] Max Landauer, Florian Skopik, Markus Wurzenberger, and Andreas Rauber. 2022. Dealing with security alert flooding: using machine learning for domain-independent alert aggregation. *ACM Transactions on Privacy and Security* 25, 3 (2022).

[27] In Lee. 2021. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons* 64, 5 (2021).

[28] Wenjuan Li, Weizhi Meng, and Lam For Kwok. 2021. Surveying trust-based collaborative intrusion detection: state-of-the-art, challenges and future directions. *IEEE Communications Surveys & Tutorials* 24, 1 (2021).

[29] Earl D Matthews, Harold J Arata III, and Brian L Hale. 2016. Cyber situational awareness. *The Cyber Defense Review* 1, 1 (2016).

[30] Reza Montasari, Fiona Carroll, Stuart Macdonald, Hamid Jahankhani, Amin Hosseinian-Far, and Alireza Daneshkhah. 2021. Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. *Digital forensic investigation of internet of things (IoT) devices* (2021).

[31] Maxwell Montgomery. 2018. Proliferation of cyberwarfare under international law: virtual attacks with concrete consequences. *S. Cal. Interdisc. LJ* 28 (2018).

[32] Tamsin Moye, Reginald Sawilla, Rodney Sullivan, and Philippe Lagadec. 2015. Cyber defence situational awareness demonstration/request for information (RFI) from industry and government (co-14068-mncd2). *NCI Agency Acquisition* (2015).

[33] Nataliia Neshenko, Christelle Nader, Elias Bou-Harb, and Borko Furht. 2020. A survey of methods supporting cyber situational awareness in the context of smart cities. *Journal of Big Data* 7 (2020).

[34] Office of the Under Secretary of Defense for Research and Engineering. 2023. *Department of Defense Mission Engineering Guide*. Technical Report. Department of Defense.

[35] North Atlantic Treaty Organisation. 2013. *BI-SC COLLECTIVE TRAINING AND EXERCISE DIRECTIVE (CT&ED) 075-003*. Technical Report. NATO.

[36] Manisha Parmar and Alberto Domingo. 2019. On the Use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander's Understanding of the Adversary. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE.

[37] Jouni Pöyhönen, Viivi Nuojua, Martti Lehto, and Jyri Rajamäki. 2019. Cyber situational awareness and information sharing in critical infrastructure organizations. (2019).

[38] Jouni Pöyhönen, Jyri Rajamäki, Harri Ruoslahti, and Martti Lehto. 2020. Cyber situational awareness in critical infrastructure protection. *Annals of Disaster Risk Sciences: ADRS* 3, 1 (2020).

[39] Attia Qammar, Jianguo Ding, and Huansheng Ning. 2022. Federated learning attack surface: taxonomy, cyber defences, challenges, and future directions. *Artificial Intelligence Review* 55, 5 (2022).

[40] NATO Science and Technology Organization. 2015. *Guideline on Scenario Development for (Distributed) Simulation Envionments - STO-TR-MSG-086-Part-II*. Technical Report. NATO STO. https://doi.org/10.14339/STO-TR-MSG-086-Part-II

[41] Johan Sigholm. 2013. Non-state actors in cyberspace operations. *Journal of Military Studies* 4, 1 (2013).

[42] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security* 60 (2016).

[43] Bart Smedts. 2010. NATO's Critical Infrastructure Protection and Cyber Defence. *Royal High Institute for Defence Center for Security and Defence Studies* (2010).

[44] Elochukwu Ukwandu, Mohamed Amine Ben Farah, Hanan Hindy, David Brosset, Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. 2020. A review of cyber-ranges and test-beds: Current and future trends. *Sensors* 20, 24 (2020).

[45] European Union. 2023. *NEWSROOM*. Technical Report. EU.

[46] David A Wallace and Shane R Reeves. 2019. Protecting critical infrastructure in cyber warfare: Is it time for states to reassert themselves? *UC Davis L. Rev.* 53 (2019).

[47] Muhammad Mudassar Yamin and Basel Katt. 2022. Use of cyber attack and defense agents in cyber ranges: A case study. *Computers & Security* 122 (2022).

[48] Robert Zager and John Zager. 2017. OODA loops in cyberspace: A new cyber-defense model. *J. Article* 21, 12 (2017).