Sharing of Cyber Threat Intelligence between States*

Philipp Kuehn, Thea Riebe, Lynn Apelt, Max Jansen, Christian Reuter

Abstract: Threats in cyberspace have increased in recent years due to the increment of offensive capabilities by states. Approaches to mitigate the security dilemma in cyberspace within the UN are deadlocked, as states have not been able to achieve agreements. However, from the perspective of IT-Security, there are Cyber Threat Intelligence (CTI) platforms to share and analyze cyber threats for a collective crisis management. To investigate, if CTI platforms can be used as a confidence-building measure between states and international organizations, we portray current CTI platforms, showcase political requirements, and answer the question of how CTI communication may contribute to confidence-building in international affairs. Our results suggest the need to further develop analytical capabilities, as well as the implementation of a broad social, political, and legal environment for international CTI sharing.

Keywords: Cyber Threat Intelligence, confidence-building measures, cyberspace, International System
Schlagwörter: Informationen zu Cyberbedrohungen, Maßnahmen der Vertrauensbildung, Cyberraum, internationales System

1. Introduction

Incidents in cyberspace have increased in the last decade (Symantec Corporation, 2019). The tremendous use of cloud services, mobile computing, and Internet of Things (IoT) add to this pressure, even between states. Given the cyberspace's militarization with state-owned cyber weapons like Stuxnet (Falliere et al., 2011) or NotPetya (McQuade, 2018), and an associated cyber security dilemma (Buchanan, 2017), some observers warn of the dangers the competition for digital supremacy and a conjoint cyber arms race could bring (Pawlak, 2016). Hence, there is a growing demand for cyber threat intelligence (CTI) sharing and IT peace research by experts to support the management of threat indicators within organizations and the IT security community (Dandurand & Serrano, 2013; Reuter, 2020; Skopik et al., 2016, 2018). Such CTI sharing would increase the cyber situational awareness (CSA) of all participants to be able to react to threats in a timely manner (Páhi et al., 2017). Even if there are ways to decrease the aforementioned tension in the international system, however not yet in cyberspace. Confidence-building measures (CBMs) have shown to be a well suited operational measure to decrease the strains between hostile states, even in times of conflict, since they are a voluntary measure (Meyer et al., 2015). They support mutual communication and cooperation on the operational level, below the political level. CBMs date back to 1975 with the OSCE's Helsinki Final Act and have been established in its current form by the OSCE's Vienna Document in 1990. They are a tool that aim to provide transparency on military doctrines, resources by improved communication and contacts between government officials. As a result, they contribute to stability, transparency and a restrain of offensive behavior (Pawlak, 2016). Other options to decrease the instability, and with it, possible conflicts, are multilateral arms-control treaties. But the negotiations for such treaties are currently deadlocked, partly due to the difficulties to agree on a definition of cyber weapons (Dickow et al., 2015). This deadlock of the top-down approach to find agreeable definitions and procedures leads to the increase of unregulated cyber operations by states, as there are little restrains not to.[1] As a result, the security of critical national infrastructure (CNI) remains highly at risk. However, as CBMs in other security-critical areas such as nuclear technology have shown (Altmann, 2019), this problem can be approached by initiating a bottom-up approach from the operational and technical perspective, which combines the organizational and technical approaches of IT-Security and CBMs. Respective international efforts for collaboration to simultaneously face threats are a vibrant topic that will be of key importance for the coming decade (Mohaisen et al., 2017).

Already, organizations collect, analyze and sometimes share cyber threat information. Cyber threat information is any information which can "help an organization identify, assess, monitor, and respond to cyber threats" (Johnson et al., 2016). They must be (i) relevant, (ii) timely, (iii) accurate, (iv) complete, and (v) ingestible, *i.e.*, they must be actionable (ENISA, 2015). Through sharing such information, organizations can improve their own security postures, as well as those of other organizations (Johnson et al., 2016). Thus, states exchanging such information would have similar benefits. Sharing, processing, and analyzing threat information is done in so-called CTI platforms, which are either federated platforms, *i.e.*, hosted by each organization itself, offering an interface for exchanging their information with each other, or used as a platform-as-a-service, *i.e.*, running in the cloud. They differ from simple data-warehouses based on their analytical capabilities, which mitigate or even remove the potential of information overload (Kaufhold et al., 2019). Shortcomings of such platforms have been discussed in prior work (Sauerwein et al., 2017; Skopik, 2016). Furthermore, developing a CTI platform faces diverse challenges, such as a lacking common terminology (Pawlak, 2016), privacy issues, as well as the reluctance by states to share security-related information (Badsha et al., 2019). Nonetheless, CTI sharing is a vital ingredient for a more secure cyberspace: due to (i) the edge of states knowing of upcoming cyber threats and (ii) the necessary communication and associated confidence building of nations about them. Besides building confidence by communicating about current threats, the publisher of threat information offers insights into the own security by giving hints in which way a state/an entity is vulnerable to them, which in itself offers or shows trust in partners.

* This article has been double blind peer reviewed. The authors thank all (anonymous) reviewers for their helpful comments and remarks.

1 Reasons for the regulative deadlock can be found in foreign and domestic policies interests which create the cyber security dilemma (Buchanan, 2016, 2017; Dunn Cavelty, 2014).

DOI: 10.5771/0175-274X-2019-4-22

Since current CTI platforms are designed with the aim to function as inter-organizational CTI sharing tools, this article strives to answer the research question: *(i) Can CTI sharing contribute to confidence building between states, and (ii) what are technical and organizational requirements by states to use CTI sharing?* Section 2 outlines the applied research methodology. Section 3 presents our findings for platforms (Section 3.1), as well as requirements defined by academics, states, and international organizations (Section 3.2). Our evaluation of identified platforms in accordance with the obtained requirements is presented in Section 4. The concluding Section 5 highlights various approaches for future research.

2. Research Methodology

To investigate the issue at hand, a combination of scientific literature and so-called grey literate is used in the review process. Scientific literature in the fields of Cyber Studies and Research, Science and Technology Studies as well as International Intelligence and Security Studies constituted the core background for this analysis. Since cyber threat (intelligence) is a matter of academic interest, but even more a matter for the private sector such as state-employed or private IT operators, the used review process minimizes the gap between research and the private sector and provided a more comprehensive picture of state-of-the-art technology in this particular field.

The literature search was conducted using the following search engines: ACM Digital Library, IEEE Xplore Digital Library, Google Scholar, and Google. The search-term deeply affiliates with the question at hand, *i.e.*, cyber (threat, exchange, platform, security, intelligence), cyber sharing (platform, tool), and cyber (space, warfare) confidence (building). Using these search terms, we used a snowball sampling technique to identify relevant literature in this field and drew on earlier works related to threat intelligence sharing, *e.g.*, Sauerwein et al. (2017). Handling our procedure openly allowed us to focus on search results most promising in regard to inter-state CTI sharing.

Using this method, we identified 40 relevant CTI platforms (see Table 1) as well as requirements for CTI sharing (platforms) as possible CBMs measures in inter-state cyberspace covering both the scientific and political field. All requirements were deduced from the obtained sources as well as official documents by regional, bi- and multilateral arrangements (see Section 4.2).

This material was used as a starting point for our investigation into current CTI sharing platforms and their potential use for confidence building between states. Similar to Sauerwein et al. (2017), we analyzed our platform sample according to a variety of perspectives, *e.g.*, (i) use cases, (ii) supported threat intelligence constructs, (iii) collaboration capabilities, and (iv) level of analysis. Additionally, we applied a list of certain criteria with special importance for inter-state confidence building (see Section 3.3).

In this context, we analyzed the sample on how the included platforms comply with the identified criteria and evaluate their potentials as tools for interstate confidence building in cyberspace (see Section 5).

Table 1: Identified platforms/data-/tool-sets

Name	Acronym	Free-to-use	Open-source	maintained	selection
Accenture Cyber Intelligence Platform				✓	
Anomali Threat Platform				✓	
Anubis Networks Cyberfeed				✓	
Automated Indicator Sharing	AIS	✓		✓	
AutoShun		✓		✓	
Barncat		✓		✓	
Bearded Avenger	BA	✓	✓	✓	✓
Blueliv Threat Exchange Network		✓		✓	
CheckPoint Cyber Security Management				✓	
Cisco Talos		✓		✓	
ClowdStrike FalconX				✓	
Collaborative Research into Threats	CRITs	✓	✓	✓	✓
Collective Intelligence Framework	CIF	✓	✓		
Cyber Defense Data Exchange and Collaboration Infrastructure	CDXI				
Cybersecurity Information Exchange Framework (X.1500)	CYBEX				
Cysiv Cyber Threat Exchange	Cysiv			✓	
Cyveillance LookingGlass Scout Prime	scout-PRIME			✓	
Defense Security Information Exchange	DSIE			✓	
Eclectiv IQ				✓	
Facebook Threat Exchange		✓		✓	
HP ThreatCentral					
IBM X-Force Exchange				✓	
Threat Intel feeds and Message Queueing system	IntelMQ	✓	✓	✓	✓
Infoblox Threat Intelligence		✓		✓	
Last Quarter Mile Toolset	LQMT	✓	✓		
Malstrom		✓	✓		
Malware Information Sharing Platform	MISP	✓	✓	✓	✓
MANTIS Management Framework		✓	✓		
McAfee Threat Intelligence Exchange		✓		✓	
Megatron		✓	✓		
Microsoft Interflow					
Nippon-European Cyberdefense-Oriented Multilayer threat Analysis	NECOMA	✓	✓		
Open Threat Exchange	OTX	✓		✓	
PassiveTotal		✓		✓	
Recoreded Future				✓	
Retail and Hospitality Information Sharing and Analysis Center	RH-ISAC			✓	
Soltra Edge		✓		✓	
ThreatConnect				✓	
ThreatQuotient				✓	
ThreatTrack ThreatIQ				✓	

3. Approaches for Cyber Threat Intelligence Sharing

Our research is driven by the motivation to discuss the question if CTI sharing tools can contribute to inter-state confidence building and, if so, what are the requirements to do so. Thereby, it is our objective to apply a broader understanding of cyber

threats. Section 3.1 introduces confidence-building measures as an approach of international politics for preventive crisis management between states. Section 3.2 presents identified tools and platforms, and Section 3.3 identifies requirements for such tools by states and international organizations.

3.1 Confidence-Building Measures as Communication and Cooperation

Confidence-building measures are instruments "which aim to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis situation. CBMs achieve this by establishing practical measures and processes for (preventive) crisis management between States." (Ziolkowski, 2013, p. 5) These measures support transparency, cooperation and stability (ibid, p. 12). However, introducing binding CBMs or any other norms in cyberspace has been difficult, because states could not agree on definitions of central concepts. Thus, the debate on CBMs has been linked to development of norms on state behavior (Pawlak, 2016).

Even though CTI is not addressing the question of behavioral norms, and what states might define as cyber hostility, CTI platforms contribute to the aspects of cooperation and transparency between states, as they enable regular and structured exchange of incoming threats and possibly unknown vulnerabilities, and offer an insight into a state's IT infrastructure. In this manner, it is possible to improve the state's individual crisis management by cooperation, transparency and exchange, which is exactly what CBMs aim for when used in international policy. CTI is increasingly used as part of public and private cyber awareness and defense (Skopik et al., 2016; Skopik et al., 2018), states, such as the US and Germany and even international organizations like NATO already use CTI databases (Dulaunoy et al., 2019; Strobel, 2015). The question is, which requirements the existing CTI platforms need to fulfill in order to become part of a bi- and multilateral exchange on cyber threats.

3.2 Platform Selection

CTI sharing platforms are a mandatory part in today's approaches for better inter-state confidence building in cyberspace. We limit ourselves to open-source and maintained platforms, due to the open innovation capabilities of the IT community. Table 1 gives information about CTI platforms, identified using the research methodology described in Section 2. There are several platforms which are provided free-to-use, while most are closed-source and only few are released under an open-source license. Due to our limitations, only four platforms remain relevant for further investigation, namely:

- Bearded Avenger (BA, 2019)
- Collaborative Research into Threats (CRITs, 2016)
- Threat Intel feeds and Message Queueing system (ENISA, 2019)
- Malware Information Sharing Platform (MISP, 2018)

3.3 Requirement Selection

Requirements aiming to increase threat intelligence sharing and according platforms can be identified in two domains, *i.e.*, the scientific and the political domain. Both provide theoretical and practical requirements related to functionality, usability, and security. In this section we cover both domains to give a comprehensive overview on requirements oriented towards theory and practice.

Dandurand and Serrano (2013) named three fundamental requirements for CTI platforms: (i) facilitate information sharing, (ii) enable automation, and (iii) facilitate the generation, refinement, and vetting of data. Those build the core of CTI platforms and will not be listed as separate requirements in our requirement selection. Sauerwein et al. (2017) identified several key findings, which their surveyed CTI platforms lacked. We use their findings to identify the difference between their revelations and ours. Their key findings state a necessity for (i) open formats for cyber threat information, (ii) built-in functionalities for data analysis, and (iii) open-source platforms. The first requirement relates to the ability of different CTI platforms to exchange their data with each other to give operators and decision makers an overview of the cyber situation. Furthermore, the formats can be discussed within the community and possibly improved in later iterations. The second requirement communicates a necessity for analysis abilities. Sauerwein et al. (2017) showed, platforms are mainly focused on data aggregation instead of data analysis, indicating that current platforms increase the information overload rather than guiding decision makers in making their infrastructures more secure. The last requirement is based on the following fact: software needs to be certified with every update to ensure compliance to security standards, *e.g.*, ISO 27001. With an open-source platform, the whole CTI platform community is able to track every update and identify possible deficiencies (Hoepman & Jacobs, 2007), decreasing the necessity for a certification.

Besides the scientific requirements, the political domain define some as well, dealing with actionable information (see Section 1) and analytical capabilities of CTI platforms. In order to extract specific requirements, we focused on documents of organizations that already established communications between states, such as the European Union (EU), Organization for Security and Co-operation in Europe (OSCE), or United Nations (UN). We ended up gathering requirements in the reports by Bourgue et al. (2013), ENISA (ENISA, 2015, 2017), OSCE (2013), and EU Directive 2016/1148 (EU, 2016).

Table 2: Results of the requirement research in the scientific (top) and political (bottom) domain.

	actionable information	open-source	open formats	compatibility	interoperability	common glossary	secured	analysis
Dandurand et al. (2013)		✓	✓					
Sauerwein et al. (2017)		✓	✓					✓
Bourgue et al. (2013)								
Directive 2016/1148 (2016)	✓	✓			✓	✓		✓
ENISA (2015, 2018)	✓	✓	✓	✓	✓	✓	✓	✓
OSCE (2013)		✓			✓	✓		

Table 2 depicts the results of the identified requirements in the scientific and political domain with relating references. The open-source and open-formats requirements are combined to a single one. Compatibility, interoperability, and a common glossary all refer to the usage of an open standard, which includes the common glossary by design. The security aspect is split into the two requirements of confidentiality and integrity, since both can be achieved by different technologies. The last derived requirement is the analytical capability of a platform.

Hence, we conclude with the following requirements being especially important for the analysis in the following section:

- open-source and open standards
- confidentiality and integrity
- analytical capabilities

4. Advancing Cyber Security through Transnational CTI Sharing

Comparing the state-of-the-art of CTI sharing platforms with the obtained requirements, this section highlights areas in which the essential needs formulated by the scientific and political domain are met.

4.1 Technical and Organizational State of the Art

Open-Source and Open Standards

Threat information must be shared in a clear and understandable manner (Howard & Longstaff, 1998). All platforms in our sample fulfill this requirement by using open standards for communication. They operate with predefined terms, as well as incident classes and types, to easily enable actors to deal with the information provided (Bodeau et al., 2018; Strom et al., 2018). Nevertheless, as the discussed literature suggests, there remains an urgent call for more harmonization of all common standards in regard to CTI sharing in general.

All platforms included in our sample feature a general characterization, thus, their potential depends mainly on the specific communities that contribute and further develop the specific platforms. The ability to gain deeper insights into the communities can be seen as a starting point for future research.

Since different actors interpret cyber events differently, a feedback element helps to manage uncertainty. This allows users to discuss the underlying issue (Serrano et al., 2014). Besides compiling information on threats in an commonly understandable way, further recommendations on how to handle them contributes to cyber security. Feedback options are included in different platforms in our sample. MISP offers a system to collaborate on events (Team CIRCL, 2017). CRITs supports comments in addition to feedback patterns integrated into the threat information format STIX (Barnum, 2014; Mitre Corporation, 2015). IntelMQ offers a harmonized structure to communicate threats, however, there is no way to comment directly or share solutions to threats (IntelMQ, 2019). Bearded Avenger does not offer this feature.

Confidentiality and Integrity

When considering how CTI can contribute to confidence building between states, there are different practical issues. First of all, the success of each CTI platform depends mainly on the willingness of its community to share threat information. As advanced approaches, mainly by the EU, Organization for Economic Co-operation and Development (OECD), and North Atlantic Treaty Organization (NATO), show, willingness tends to be stronger among parties that have a common history and stable framework for communication. Besides a lack of political will, there can be restrictions due to an organization's limited availability of free resources or adequately skilled employees (Sauerwein et al., 2017). In regard to CTI sharing, such political willingness depends not only on the general trust and confidence among all parties involved, but to a similar degree on the trust the parties have regarding the reported cyber incidents covered on the platform. Therefore, there are two dependencies of trust, *i.e.*, the platform user's trust towards the provider and vice-versa (Sauerwein et al., 2017). Inserting malicious CTI data into the platform makes its users possibly insecure. Hence, the trust between users and providers is of critical importance. This also includes the trust in the storage of platforms, *i.e.*, the confidentiality and integrity of stored data. All selected platforms use open-source database implementations to store their data. Hence, every provider can compare his / her security criteria against the available source-code.

Analytical Capabilities

It is important for every single actor within a community to contribute to CTI platform development and improve its analytical capabilities. Only analytical advancements distinguish CTI platforms from pure data collection (Bourgue et al., 2013).

Analytical capabilities include categorization and ranking of threats, as well as automated prioritization. IntelMQ is equipped with the most favorable potentials for CTI sharing, as such capabilities are most developed on this specific platform. Its analytical features are implemented using third-party implementations, so-called bots. They can be stacked and nested together to build an analysis framework. Hence, the quality of analytical capabilities of IntelMQ depends on the quality of the available bots. MISP offers interfaces to analyze the available data with external tools, using a so-called MISP SEC-Ops System (MISP, 2018). But there are no integrated analytics capabilities in MISP. CRITs and Bearded Avenger offer no way to integrate external tools into the platform's workflow.

Table 3: Fulfillment of requirements per platform. A tick denotes the platform fulfills the requirement. A circle denotes partially fulfillment (e.g. with use of third-party applications). A cross denotes the platform does either not fulfill the requirement or there is limited to no documentation about it.

Name	BA	CRITs	IntelMQ	MISP
analytical capabilities	✗	✗	○	○
automatic communication of current threats	✓	✓	✓	✓
confidentiality and integrity of the platform	○	○	○	○
open-source	✓	✓	✓	✓
open standards	✗	✓	○	✓

Table 3 depicts which requirements, elaborated in Section 4, are fulfilled by each platform, showing that there is no state-of-the-art open-source CTI platform that is able to fulfill all requirements stated by states, international organizations, and academia.

4.2 Additional Findings

While this article strives to explore questions investigating technical and organizational issues connected to transnational CTI sharing, we want to highlight the importance of social and theoretical concerns. They are especially relevant when it comes to future academic research and are not yet elaborated in the field of inter-state confidence building focusing on CTI sharing.

CTI is mainly about human intelligence and as with all technological changes, this will not take place by simply adopting new technical frameworks or designs. Adopting effective information-sharing techniques through such channels might provide information on secure cyber behavior. However, without a greater socio-political and legal environment facilitating their functionality, they will not be effective at all. This is why it is crucial for political decision makers to closely follow trends and developments, re-evaluate their policies and have an agreed procedure for modifying them, if necessary (Horizon 2020, 2017; Johnson et al., 2016).

In the field of inter-state security or CTI sharing, sensitivity is reached by creating a stable and predictable environment for the discussed measures. Political and legal arrangements build the foundations for such an environment. Embedded in a stable socio-political and legally equipped environment constituted by common frameworks and emerging international norms for appropriate state behavior in cyberspace, CTI sharing platforms can provide effective advancements in security and support international preventive crisis management (Ziolkowski, 2013). However, as the dynamics of the international strategic stability are causing a crisis in CBMs and Arms Control, CTI can be implemented even on national or regional levels as part of anti-cybercrime strategies (Skopik, 2016). As CTI will be helpful with communication and cooperation aspects for confidence building, the implications for a future cyber arms control regime are unclear. Cyber arms control measures would need additional information on state-driven cyber operations, depending on the definition of cyber weapons, as well as the metrics for their measurements (Altmann & Siroli, 2018; Reinhold & Reuter, 2019; Ziolkowski, 2013). However, CTI can be a part of an attribution regime, which would collect technical indicators for cyber attribution and IT forensics (Davis et al., 2017).

Furthermore, any kind of information sharing is faced with a liability issue: When actors in an information-sharing community know about a potential threat (for example, by receiving feeds from this particular community), they have to secure their own capability to address this particular threat in a suitable way. Otherwise, they might find themselves confronted with the question, why they did not take appropriate action before this particular threat started to materialize. Omitted action might prove especially relevant in the context discussed here, since CTI sharing between states is not only connected to international security, but similarly to domestic security, especially for critical infrastructures (critIS) managed and secured by governmental bodies. As numerous incidents in the past, *e.g.*, the Baltimore Fallout in early 2019 (Liptak, 2019) or US digital incursions into Russia's electric power grid (Perlroth & Sanger, 2019), proved that public infrastructures are possible targets for cyber-attacks. Due to their unique social and political nature, omitted actions are of special importance when it comes to (de-)escalating a bi-, regional, or international conflict. Hence, analytical capabilities of CTI sharing platforms have to be as high as possible, while their coverage should be regional or even global to be effective. As these remarks suggest, improvements that go beyond the pure technical nature of CTI sharing are of high importance on every level within the sharing community.

5. Conclusion and Future Work

Today's increase of large scale cyber operations by organized criminal groups or even political actors (Reuter, 2019) demand new forms of cross-organizational and international sharing of information to discover cyber threats at an early state on and enable an early warning infrastructure (Skopik et al., 2016). States collect threat information, and sharing them to gain a large-scale cyber situational awareness would contribute to an increase in trust and security. As the risk of unintended collateral damage or even conflict remains as long as states have more incentives to behave offensive than defensive in cyberspace (Buchanan, 2017; Dunn Cavelty, 2014), we suggest to use CTI as a tool for confidence building between states. CBMs support communication and cooperation on an operational level, and help to increase stability. Due to the obstacles to define the term of cyber weapons internationally (Dickow et al., 2015), CTI focusses on the improvement of information sharing and cooperation, thus providing situational awareness and support of common understandings of threats. As an instrument, CTI platforms can serve as a tool for preventive crisis management and IT forensics in an attribution regime (Davis et al., 2017). Therefore, we answered the question, whether or not CTI platforms can be used as CMB, followed by a literature review of the field of available CTI platforms and the field of states and inter-state organizations and identified requirements for (i) open-source and open standards, (ii) confidentiality and integrity, and (iii) analytical capabilities. We matched the identified platforms, their features and the obtained requirements against each other. Our results suggest that many CTI platforms lack further analytical capabilities as suggested in prior work (Sauerwein et al., 2017). In order for technical improvements to take further effect, the evolution of a broader social, political, and legal environment for international CTI sharing is crucial. Hence, we suggest future work on the analytical capabilities of CTI platforms, open standards and definitions for a common understanding, as well as the general evolution of a supportive socio-political environment.

6. Acknowledgements

This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE as well as the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 CROSSING – 236615297.

Philipp Kuehn is a PhD researcher at the Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at Technische Universität Darmstadt. His research focuses on cyber security, attribution and vulnerability disclosure, as well as threat communication.

Thea Riebe is a PhD researcher at the Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at Technische Universität Darmstadt. Her research focusses on cyber security, dual-use and technology assessment.

Lynn Apelt is a student at the master's program of International Studies / Peace and Conflict Studies at the Goethe University Frankfurt and the Technical University of Darmstadt.

Max Jansen is a student at the master's program of International Studies / Peace and Conflict Studies at the Goethe University Frankfurt and the Technical University of Darmstadt. His research focuses on (post-) conflict dynamics, the role of civil society, as well as questions of cyber security and gender.

Christian Reuter is Full Professor for Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at the Technische Universität Darmstadt with a secondary appointment in the Department of History and Social Sciences. His research focuses on interactive and collaborative technologies in the context of crises, security, safety, and peace.

7. Bibliography

Altmann, Jürgen. (2019). Confidence and Security Building Measures for Cyber Forces. In *Information Technology for Peace and Security* (pp. 185–203). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4_9

Altmann, Jürgen, & Siroli, Gian Piero. (2018). Confidence and Security Building Measures for the Cyber Realm. In A. Masys (Ed.), *Handbook of Security Science*. London: Routledge.

BA. (2019). Bearded Avenger. Retrieved June 19, 2019, from https://github.com/csirtgadgets/bearded-avenger

Badsha, Shahriar, Vakilinia, Iman, & Sengupta, Shamik. (2019). Privacy preserving cyber threat information sharing and learning for cyber defense. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019* (pp. 708–714). IEEE. https://doi.org/10.1109/CCWC.2019.8666477

Barnum, Sean. (2014). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). *MITRE Corporation*, *July*, vol. *11*, , pp. 1–20. Retrieved from http://blackberry8520.b277.doihaveamobilestrategy.com/http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0_(Draft).pdf

Bodeau, Deborah J., Mccollum, Catherine D., & Fox, David B. (2018). "Cyber Threat Modeling: Survey, Assessment, and Representative Framework"," PR 18-1174. *HSSEDI, The Mitre Corporation*, iss. 18. Retrieved from https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf

Bourgue, Romain, Budd, Joshua, Homola, Jachym, Wlasenko, Michal, & Kulawik, Dariusz. (2013). Detect , SHARE , Protect Solutions for Improving Threat Data Exchange among CERTs. *European Network and Information Security Agency (ENISA)*, iss. October, pp. 51. Retrieved from https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

Buchanan, Ben. (2016). *The Cybersecurity Dilemma*. London: C. Hurst & Co.

Buchanan, Ben. (2017). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. London: C. Hurst & Co. https://doi.org/10.1093/acprof:oso/9780190665012.001.0001

CRITs. (2016). CRITs. Retrieved June 6, 2019, from https://crits.github.io

Dandurand, Luc, & Serrano, Oscar. (2013). Towards improved cyber security information sharing. In *International Conference on Cyber Conflict, CYCON* (pp. 1–16).

Davis, John S. II, Boudreaux, Benjamin, Welburn, Jonathan William, Ogletree, Cordaye, McGovern, Geoffrey, & Chase, Michael S. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace*.

Dickow, Marcel, Hansel, Mischa, & Mutschler, Max M. (2015). Präventive Rüstungskontrolle – Möglichkeiten und Grenzen mit Blick auf die Digitalisierung und Automatisierung des Krieges. *Sicherheit & Frieden*, vol. *33*, iss. 2, pp. 67–73. https://doi.org/10.5771/0175-274x-2015-2-67

Dulaunoy, Alexandre, Iklody, Andras, Dereszowski, Andrzej, Studer, Christian, Vandeplas, Christophe, Andre, David, … Clement, Steve. (2019). *Malware Information Sharing Platform*.

Dunn Cavelty, Myriam. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, vol. *20*, iss. 3, pp. 701–715. https://doi.org/10.1007/s11948-014-9551-y

ENISA. (2015). *Actionable Information for Security Incident Response*. Retrieved from https://www.enisa.europa.eu/publications/actionable-information-for-security

ENISA. (2017). *Information Sharing and Analysis Centres (ISACs) Cooperative models*. https://doi.org/10.2824/549292

ENISA. (2019). *Incident Handling Automation*. *Community Projects*. Retrieved from https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

EU. (2016). Directive (EU) 2016 / 1148. *Official Journal of the European Union*, vol. *6*, iss. 1, pp. 30. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Falliere, Nicolas, Murchu, Liam O., & Chien, Eric. (2011). W32. stuxnet dossier. *Symantec Security Response*, vol. *14*, iss. February, pp. 1–69. Retrieved from http://large.stanford.edu/courses/2011/ph241/grayson2/docs/w32_stuxnet_dossier.pdf

Hoepman, Jaap Henk, & Jacobs, Bart. (2007). Increased security through open source. *Communications of the ACM*, vol. *50*, iss. 1, pp. 79–83. https://doi.org/10.1145/1188913.1188921

Howard, John D., & Longstaff, Thomas A. (1998). *A common language for computer security incidents*. *Sandia National Laboratories*. https://doi.org/10.2172/751004

IntelMQ. (2019). IntelMQ – Data Harmonization. Retrieved June 26, 2019, from https://github.com/certtools/intelmq/blob/develop/docs/Data-Harmonization.md

Johnson, Christopher S., Badger, Mark Lee, Waltermire, David A., Snyder, Julie, & Skorupka, Clem. (2016). *Guide to Cyber Threat Information Sharing*. *Special Publication – Council for Agricultural Science and Technology*. Gaithersburg, MD. https://doi.org/10.6028/nist.sp.800-150

Kaiafas, Georgios (European Commission). (2017). *Horizon 2020. Threat Intelligence Sharing : State of the Art and Requirements*. Retrieved from https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D5.1-E-0517-Threat-Intelligence-Sharing.pdf

Kaufhold, Marc-André, Rupp, Nicola, Reuter, Christian, & Habdank, Matthias. (2019). Mitigating Information Overload in Social Media during Conflicts and Crises: Design and Evaluation of a Cross-Platform Alerting System. *Behaviour & Information Technology (BIT)*.

Liptak, Andrew. (2019, May 25). Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems. *The Verge*. Retrieved from https://www.theverge.com/2019/5/25/18639859/baltimore-city-computer-systems-cyberattack-nsa-eternalblue-wannacry-notpetya-cybersecurity

McQuade, Mike. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, pp. 1–6. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Meyer, Berthold, von Bredow, Wilfried, & Evers, Frank. (2015). 40 Jahre Schlussakte von Helsinki, 25 Jahre Pariser Charta: Rückblick und Ausblick auf die OSZE. *Sicherheit & Frieden*, vol. *33*, iss. 2, pp. 106–111. https://doi.org/10.5771/0175-274x-2015-2-106

MISP. (2018). *MISP – User Guide, A Threat Sharing Platform*. MISP Community. https://www.circle.lu/doc/misp/

Mitre Corporation. (2015). Collaborative Research Into Threats. *MITRE Corporation*. Retrieved from https://crits.github.io/.

Mohaisen, Aziz, Al-Ibrahim, Omar, Kamhoua, Charles, Kwiat, Kevin, & Njilla, Laurent. (2017). Rethinking information sharing for threat intelligence [Position Paper]. *HotWeb 2017 – Proceedings of the 5th ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies*, pp. 1–7. https://doi.org/10.1145/3132465.3132468

OSCE. (2013). Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. *DEC/1202*, vol. *10*, iss. December, pp. 4. Retrieved from http://www.osce.org/pc/109168?download=true

Páhi, Tímea, Leitner, Maria, & Skopik, Florian. (2017). Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy* (Vol. 2017, pp. 334–345). SCITEPRESS – Science and Technology Publications. https://doi.org/10.5220/0006149703340345

Pawlak, Patryk. (2016). Confidence-Building Measures in Cyberspace : Current Debates and Trends. *International Cyber Norms: Legal, Policy & Industry Perspectives*, vol. *20*, iss. April 2015, pp. 129–153.

Perlroth, N., & Sanger, D. E. (2019). U.S. Escalates Online Attacks on Russia's Power Grid – The New York Times. *New York Times*. The New York Times Company. Retrieved from https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html%0Ahttps://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?smid=nytcore-ios-share

Reinhold, Thomas, & Reuter, Christian. (2019). Arms Control and its Applicability to Cyber Space. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 207–233). Wiesbaden: Springer.

Reuter, Christian. (2019). Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. (C. Reuter, Ed.). Wiesbaden. Retrieved from https://doi.org/10.1007/978-3-658-25652-4

Reuter, Christian. (2020). Towards IT Peace Research: Challenges on the Interception of Peace and Conflict Research and Computer Science. *S+F Sicherheit Und Frieden / Peace and Security*, vol. *38*, iss. 1, pp. 1–15.

Sauerwein, Clemens, Sillaber, Christian, Mussmann, Andrea, & Breu, Ruth. (2017). Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)* (pp. 837–851).

Serrano, Oscar, Dandurand, Luc, & Brown, Sarah. (2014). On the Design of a Cyber Security Data Sharing System. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security – WISCS '14* (Vol. 2014-Novem, pp. 61–69). New York, New York, USA: ACM Press. https://doi.org/10.1145/2663876.2663882

Skopik, Florian, Páhi, Tímea, & Leitner, Maria (Eds.). (2018). *Cyber Situational Awareness in Public-Private-Partnerships*. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56084-6

Skopik, Florian, Settanni, Giuseppe, & Fiedler, Roman. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, vol. *60*, , pp. 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Strobel, Warren. (2015, February 10). U.S. creates new agency to lead cyberthreat tracking – Reuters. *Reuters*. Retrieved from https://www.reuters.com/article/us-cybersecurity-agency/u-s-creates-new-agency-to-lead-cyberthreat-tracking-idUSKBN0LE1EX20150210

Strom, Blake E., Applebaum, Andy, Miller, Doug P., Nickels, Kathryn C., Pennington, Adam G., & Thomas, Cody B. (2018). MITRE ATT&CK – Design and Philosophy. *Technical Report*, iss. July, pp. 37.

Symantec Corporation. (2019). Symantec Internet Security Threat Report. *Network Security*, iss. 24, pp. 61. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Team CIRCL. (2017). MISP features and functionalities. Retrieved June 25, 2019, from https://www.misp-project.org/features.html

Ziolkowski, Katharina. (2013). Confidence Building Measures for Cyberspace–Legal Implications. *NATO CCD COE Publication*, pp. 1–88.