Weber, Hannah-Sophie:

Multilateral Approaches to Cyber Security Capacity Building: The Rise of Non-Traditional Actors.

Bachelorarbeit, Wintersemester 2022

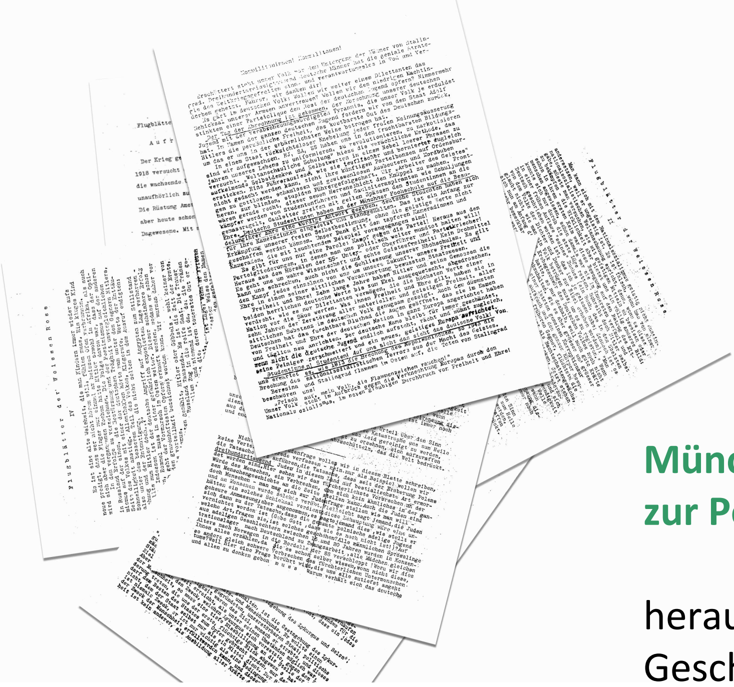
Sozialwissenschaftliche Fakultät

Ludwig-Maximilians-Universität München

https://doi.org/10.5282/ubm/epub.91373

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT



Münchener Beiträge zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2022

Hannah-Sophie Weber

Multilateral Approaches to Cyber Security Capacity Building: The Rise of Non-Traditional Actors.

Bachelorarbeit bei
Prof. Dr. Andreas Kruck
2021

Abstract

This thesis presents a qualitative empirical analysis of explanatory causal mechanisms for the rise of non-traditional actors (NTAs) in multilateral Cyber Security Capacity Building (CSCB). Within the framework of an Explaining-Outcome Process Tracing, three conjectures are derived from Organisational Ecology and Historical Institutionalism. The elaborated approach merges complementary structural and agency-centred causal mechanisms. Case-specific events and scope conditions further specify these conjectures. This study finds that the rise of NTAs is shaped by their flexibility to choose favourable niches, their beneficial interaction with traditional actors, and finally, their perception as an opportunity to realise interests by traditional actors. Further research could pursue an adjuvant quantitative approach for testing the conjectures among a broader range of actors. That said, the rise of NTAs comes with far-reaching implications for traditional actors, such as Germany, in CSCB and the future of multilateral approaches in cyberspace itself. This is closely tied to the concluding impetus for international coordination, a common aim and efficient public-private cooperation in CSCB.

Keywords: *Cyber Security Capacity Building; Non-Traditional Actors; Non-State Actors; Multi-Stakeholder Governance; Public-Private Cooperation; Multilateralism*

Table of Contents

Acronyms

AU	African Union
ASEAN	Association of Southeast Asian Nations
BSI	German Federal Office for Information Security
CEPI	Coalition for Epidemic Preparedness Innovations
CMM	Cybersecurity Capacity Maturity Model
CoE	Council of Europe
CRI	Cyber Risk Institute
CSCB	Cyber Security Capacity Building
DDP	Digital Development Partnership
DV	Dependent Variable
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUISS	European Institute for Security Studies
FDP	Free Democratic Party (Germany)
FIRST	Forum of Incident Response and Security Teams
GCFE	Global Center for Cyber Expertise
GCSC	Global Commission on the Stability of Cyberspace
GCSCC	Oxford Global Cyber Security Capacity Centre
GPD	Global Partners Digital
HI	Historical Institutionalism
HP	Hewlett-Packard
ICT(s)	Information and Communication Technologies
IGO(s)	Intergovernmental Organisation(s)
IMF	International Monetary Fund
(I)NGO	(International) Non-Governmental Organisation
IO	International Organisation
ITU	International Telecommunications Union
IV	Independent Variable
NATO	North Atlantic Treaty Organisation
NTA(s)	Non-Traditional Actor(s)
OAS	Organisation of American States
OE	Organisational Ecology
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Co-operation in Europe
SPD	Social Democratic Party of Germany
UK	United Kingdom
UN	United Nations
UN GGE	United Nations Group of Governmental Experts
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime
UN OEWG	United Nations Open-Ended Working Group
US	United States of America
WBG	World Bank Group

1. Introduction

“We strengthen digital civil rights and IT security. Ensuring them is a state duty […] The cybersecurity strategy and IT security law will be advanced. In addition, we are safeguarding digital sovereignty.”

SPD, Greens, & FDP (2021, p. 16)

Cybersecurity has evolved from a technical expert issue (Malcolm, 2017) to a matter of the highest political relevance. Originally of economic concern, it soon transferred to human rights and, more recently, international development (Klimburg & Zylberberg, 2015). Cyberspace has transformed both economic and social affairs in the 21st century. The global sensitisation for security in cyberspace likewise increased. Cybersecurity is an integral part of national and international security strategies, defence doctrines, and foreign policies today. This relevance for national and international politics has most recently been emphasised by the brand-new coalition agreement of the Social Democratic Party of Germany (SPD), the Greens, and the German Free Democratic Party (FPD). The networked and borderless nature of cyberspace turns cyber risks into a global problem. Incentives to maliciously exploit networks continue to multiply.

COVID-19 rapidly shifted most aspects of our lives online. The amplified digital connectivity exposes vulnerabilities of public and private actors alike. Consequently, the need to advance cybersecurity capacities rises (Bei, 2020). With increasing cybercrime, cyber-espionage, cyber-weapons and terrorism, securing cyberspace and reliant infrastructures presents a significant concern for all stakeholders (Eggenschwiler, 2018). Developing and developed nations are exposed and often unable to manage cyber-attacks. Witnessing the rising number of developing countries experiencing digitisation, addressing these threats constitutes an international security priority. Cyberspace is of the highest scholarly interest, as it involves and blurs core concepts such as borders, state interactions or national sovereignty (Broeders, 2017). The unique nature of cyberspace, namely its decentralisation, worldwide interconnectedness, and intertwined layers, makes it particularly resistant to traditional governance tools of state actors (Waz & Weiser, 2012). Reciting Valeriano and Maness (2018, p. 259), „the importance of cyber security as an emerging issue in International Relations cannot be overstated.“ As a mechanism enabling states and organisations to assist each other in protecting peace and stability in cyberspace, Cyber Security Capacity Building (CSCB) emerged in the mid-2000s (Collett, 2021). CSCB is considered a key instrument that connects the various discourses and plays an increasing role in foreign policy (Klimburg & Zylberberg, 2015). CSCB can be defined as a way to „empower individuals, communities, and governments to achieve their developmental goals by reducing digital security risks stemming from access and use of Information and Communication Technologies" (Pawlak, 2014b, p. 5). It is perceived as a process that targets institutional and legal conditions, organisational provisions, and human resources while ultimately aiming at socio-political transformations. The variety of actors in CSCB continues to grow (see 4.). This is linked to "one of the most significant changes in the multilateral system in recent years" (Bull, Bøås, & McNeill, 2004). Namely, the considerable increase in the scale and influence of non-traditional, non-state actors' participation in the system (Bull et al., 2004). The complexity of public policy itself is elevated, as national governments, on the one hand, and multinational companies, on the other, can no longer resolve evolving challenges individually. This reconstitution is influenced by technological advancement and closely intertwined with a pluralisation of relevant, *polymorphous* (Stadnik, 2018) actors. Reciting Maurer and Nelson (2020, p. 4), "international and multi-stakeholder cooperation is not a *nice-to-have* but a *need-to-have*."

The term *non-traditional actors* (NTAs) is introduced for this thesis. It relies on the classification of governance actors in areas of limited statehood by Risse (2012), the mapping of actors in CSCB by Maurer and Nelson (2020), and the understanding of non-state actors by Kulesza and Eggenschwiler (2020). Accordingly, the term NTA comprises three sub-types of non-state actors: (1) multi-stakeholders and (international) non-governmental organisations ((I)NGOs), (2) academia, and (3) multinational enterprises.[1] All of these sub-types certainly qualify for an individual in-depth analysis. Instead of providing single case studies, however, this thesis aims to identify common threads of CSCB engagement across this inherent diversity. Defined in the negative, NTAs are actors that are not "traditional" players in international politics. Another commonality of NTAs this thesis refers to is their exclusively benevolent character and their goal to contribute to the overall global state of cybersecurity (Kulesza & Eggenschwiler, 2020). Malevolent actors are not considered for this analysis. The political awareness that building a secure cyberspace requires such non-traditional approaches continues to increase (Schnidrig & Aiken, 2020).

[1] See **Annexe 1** for a visualisation of the NTA concept.

“Thus, when we speak of multilateralism, we are not merely talking about cooperation between several states, but also about the fact that this cooperation […] is directed towards a particular goal, such as the establishment or maintenance of peace and security.”

Philipps & Braun (2020, p. 17)

The chosen approach is consistent with the (third) trend for the future of multilateralism, as defined by Philipps and Braun (2020). They delineate the emergence of new forms of international cooperation alongside traditional and established institutionalised multilateralism. NTAs gained significant influence in the past years and mounted their importance in international cooperation (Philipps & Braun, 2020). The role of such actors is among the most discussed issues within scholarly debates on globalisation (von Bernstorff, 2007; Rittberger, 2008). Philipps and Braun (2020) name the health sector as a prominent example, with actors like the Coalition for Epidemic Preparedness Innovations (CEPI), an alliance of private actors and governments. They point out how COVID-19 drew attention to the contribution of NTAs as important voices in international cooperation (Philipps & Braun, 2020). Abbott, Green, and Keohane (2016) explore the trend in climate governance. They explain how involving all relevant stakeholders is already accepted within this area, resulting in new (in-)formal multilateral cooperation formats. The field of CSCB grows with the rising complexity and scale of connected data and network volumes (School, 2021). The growing number of non-state actors in CSCB steering activities (Nasiritousi, Hjerpe, & Linnér, 2016) is somewhat mirrored by the developments in the climate governance area (Abbott, 2012; Bulkeley et al., 2012; Nasiritousi et al., 2016; Schroeder & Lovell, 2012). What makes this study on NTAs particularly interesting is a critical perspective on multi-stakeholder formats and (corporate) cyber diplomacy. This includes questioning how both multinational companies and nation-states shape their roles as (norm) entrepreneurs in cyberspace and how their CSCB efforts relate to identities and interests (Kulesza & Eggenschwiler, 2020).

NTAs are on the rise in multilateral CSCB, and as a dynamic, multi-disciplinary field, CSCB has the opportunity to create an institutional architecture suited to the evolving modalities (see 4.). While the broader topic of cybersecurity is based on a personal research background in cyberwarfare, the collaboration with the German Federal Office for Information Security (BSI) set the focus on CSCB. Divergent approaches and competing objectives may shape the future of CSCB. It may, however, also grow into an ecosystem with coordinated, shared, and aligned aims and common practices between the different CSCB actors and communities (Collett &

Barmpaliou, 2021). Researching the conjectures behind the rise of NTAs in multilateral CSCB is respectively essential. This study is designed to contribute to a more detailed understanding of changes in the CSCB ecosystem. It aims to point out implications for traditional state actors, such as Germany, for shaping their CSCB profile in regard to the rise of NTAs. This thesis provides a theory-driven analysis of changes in the multilateral CSCB ecosystem by asking:

How can the rise of non-traditional actors in multilateral Cyber Security Capacity Building be explained?

First, the theoretical framework is explained. Following this, the research design, methodology (Process Tracing) and selection of empirical data are outlined. This is complemented by an overview of actors in multilateral CSCB and the empirical analysis. Finally, the conclusion provides an overview of this study's limitations and findings.

2. Theoretical Framework

The research question is answered, following the guidelines for a theory-based empirical explanation in political science. A y-centric research design, as conceptualised by Ganghof (2019), enables the causal explanation of the dependent variable (DV). This DV is the institutional outcome in question, precisely the rise of NTAs in multilateral CSCB. The selection of independent variables (IVs), the conjectures (C1, C2), is inspired by the analysis of climate governance with an Organisational Ecology (OE) framework by Abbott et al. (2016). This research adapts the existing framework to CSCB. OE, however, cannot exhaustively address questions of organisational design and behaviour. As Abbott et al. (2016) recommend, a complementary agency-centred perspective is added to the OE perspective in a second step. This perspective (C3) is based on Historical Institutionalism (HI).

What substantiates the choice of this specific case and theories? The rise of NTAs in CSCB is selected as a *most-likely case* to demonstrate the applicability of OE theory. When the main objective is to explain causal mechanisms behind a new phenomenon, choosing such a case is appropriate (Abbott et al., 2016). This selection, however, limits generalisation. Regarding the method of Explaining-Outcome Process Tracing, it is a case selection based on the relevant outcome (Beach & Pedersen, 2012) and the interest in the conjectures leading to it. This attempt follows the impulse of Abbott et al. (2016) to establish a transfer of OE's explanatory power to domains other than climate governance. CSCB is an issue area where much new NTA activity takes place. This presents a clue for OE's sensitivity for institutional density, legitimation, and ecosystem populations (Hannan, 2005).

2.1. State of Research

Significant growth of research literature on the overarching topic of cybersecurity can be observed throughout the last decade (Clark et al., 2014; Singer & Friedman, 2014; Müller & Kremer, 2014; Austin, 2018; Tasheva, 2021). Scholars of IR sub-disciplines, prominently of security and strategic studies, increasingly research global security impacts of new technologies. Existing literature on the cybersecurity sub-topic CSCB ranges from works on policy implications and concepts (Pawlak, 2014b; Klimburg & Zylberberg, 2015; Pijnenburg Muller, 2015; Lango, 2016) to the investigation of what drives CSCB efforts (Heeks, 2014; OECD, 2015; World Economic Forum, 2012; Tiirmaa-Klaar, 2016; Pawlak, 2016a). Comparing different regions or national actors and evaluating best practices seems to be of particular interest (Schia, 2016; Nikolova, 2017; Crespo et al., 2018). CSCB efforts are measured using models such as the Cybersecurity Capacity Maturity Model for Nations (CMM) (GCSCC, 2021a) or likewise indices (Hathaway, 2013; Hathaway, 2015; ASPI, 2015; ITU, 2016). Hameed et al. (2018) drafted a high-level thematic and regional analysis of Cybil Portal project data and identified CSCB-project success factors.[2] In-depth research has also been conducted on uni- and bilateral CSCB dynamics (Radunović & Rüfenacht, 2016; Pawlak & Barmpaliou, 2017; Homburger, 2019; Dutton et al., 2019; Calderaro & Craig, 2020; Watanabe, 2020a; Collett, 2021).

Recent works, however, start shifting the focus to global capacity-building approaches (Pawlak, 2016b; Pawlak & Missiroli, 2019; Creese et al., 2021; Collett & Barmpaliou, 2021). Pawlak's (2016b) and Pawlak & Missiroli's (2019) works outline trends and challenges for international cooperation in cyberspace while considering CSCB as part of a more comprehensive assessment of trends in international cooperation on cyber issues. The cluster of research that shifts the perspective *beyond the state* explores broader implications for governance, namely *networked governance* (Dunn Cavelty & Wenger, 2019). Cyberspace itself is shaped by fragmented authorities (Ruhl et al., 2020). A related, prominent research agenda

[2] The *Cybil Portal* was launched as a global platform for the CSCB community in 2019. As an initiative of the GFCE, it is designed to provide transparent access to information on best practices for CSCB stakeholders (GCSCC, 2021b).

regards the shaping influences of global scripts and isomorphic processes on institutional design (DiMaggio & Powell, 1983; Finnemore, 1996).

The use of CSCB as a foreign policy tool has been a recurring notion in CSCB research (Pawlak, 2016b; Hohmann, Pirang & Benner, 2017). The inherent risk is that developmental agendas are impeded by Western interests and security visions that shape CSCB objectives. The identified root cause is that creating a collaborative effort around shared interests is easier (Hui et al., 2010). Traditional foreign policy interests, however, remain intrinsically different. If there were an agreement on CSCB among all countries, no foreign policy would be needed on it (Collett & Barmpaliou, 2021). Although thorough research has been carried out on CSCB, on the one hand, and OE, on the other hand, studies focusing on OE and its perspective on institutional change within the CSCB realm are to be sought.

2.2. Organisational Ecology

The constructed research design aims at the causal explanation of an institutional outcome. Process-based, structural theories emphasise the (global) environment that international institutions operate in (Voeten, 2019). This perspective contrasts with distributive or rational functionalist streams of theory. Structural process theories highlight the influence of pre-existing institutions and structures on new institutional design (Voeten, 2019). The structural process approach selected for this thesis is among the theoretical streams that currently receive increasing scholarly attention. Explaining how organisational structures evolve in response to the conditions in their environment (Hannan & Freeman, 1977; Hannan & Freeman, 1984; Hannan, 2005) is at the heart of OE. OE relies on a positivist epistemology and a structural understanding. It thereby provides a more structural account for the emergence of new forms of governance than related scholarly approaches within the historical institutionalist framework (Drezner, 2010; Fioretos, 2011; Farrell & Newman, 2014; Keohane, 2017).

Abbott et al. (2016) introduced the theory to IR to address former analytical gaps. They did so by applying OE approaches to grasp the shift from Intergovernmental Organisations (IGOs) toward private actors in climate governance (Voeten, 2019). OE focuses on the particular character of organisational populations, including their diversity, growth or decline, and the chance of survival (Abbott et al., 2016). Institutional design is thus analysed in response to the strategic, social, cultural, political, and economic environment in which actors operate.

> *"Like natural ecosystems, the cyber ecosystem comprises a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies) – that interact for multiple purposes."*
>
> **Reitinger (2011, p.2)**

Based on this understanding of a cyber ecosystem, precisely the CSCB ecosystem, OE theory is applied for the first step of the empirical analysis (C1, C2). It is used to investigate the rise of NTAs in CSCB compared to traditional (international) actors such as IGOs.

2.3. Agency-Centred Historical Institutionalism

HI is employed in a second step (C3) to explain the institutional outcome in question (the rise of NTAs in multilateral CSCB) more comprehensively. It complements the structural OE approach by bringing in agency as an additional relevant factor (Emmenegger, 2021). This improves the explanatory power of the theoretical framework and is based on the conviction that institutional change can hardly be coherently traced without considering agency (DiMaggio, 1988). Institutionalist structural approaches nonetheless emerged in contrast to dominant behavioural perspectives, and agency remains a highly debated factor among scholars (Voeten, 2019).

NTAs add complexity to the traditional structural layers of the international order and challenge conventional sources of agency (Kulesza & Eggenschwiler, 2020). According to Abbott et al. (2016), agency-centred and organisational ecology approaches are perceived as complementary rather than contradictory. OE enhances our understanding of both constraints and opportunities presented by environmental variables. Agency-centred HI theory supplies additional micro-foundations for understanding institutional responses to those conditions and purposive actions by actors to shape institutions (Abbott et al., 2016). HI claims that an institutional outcome is the result of a series of actions (Voeten, 2019). These may have been of purposive or random nature. Given the inability of existing institutions to adapt and their declining agency, actors are likely to engage in non-traditional alliances and initiatives to advance their interests (Philipps & Braun, 2020). NTAs, with their agency and capabilities, thus shape transnational governance.

3. Research Design, Method, and Data

Process tracing (PT) is selected as the method for answering the research question in accordance with the y-centric exploration of the institutional outcome. PT is prominent among researchers (Mahoney, 2012; Beach and Pedersen, 2013; Rohlfing, 2014; Bennett & Checkel, 2014; Humphreys & Jacobs, 2015). Y-centric explorations examine how complementary theories can be combined within causal mechanisms to explain a specific outcome (Ganghof, 2016). In this case, the employed theories are OE and HI, as outlined above (see 2.). The analysis is based on an entirely qualitative approach. After giving an overview of CSCB dynamics and actors, the process analysis is conducted. Selected communication by CSCB actors is considered necessary data for testing the theoretical framework (Ricks & Liu, 2018). Additionally, secondary research literature is examined. This cumulated data is retrieved online and constitutes the empirical material for elaborating on the research question via qualitative content analysis. The aim is to sharpen and – to a certain extent – test relevant causal links between theoretically derived conjectures (IVs) and the institutional outcome (DV). The PT is guided by three conjectures **(C1, C2, C3)** that comprise two steps each and result in the outcome in question (DV), the rise of NTAs in multilateral CSCB.

3.1. Process Tracing

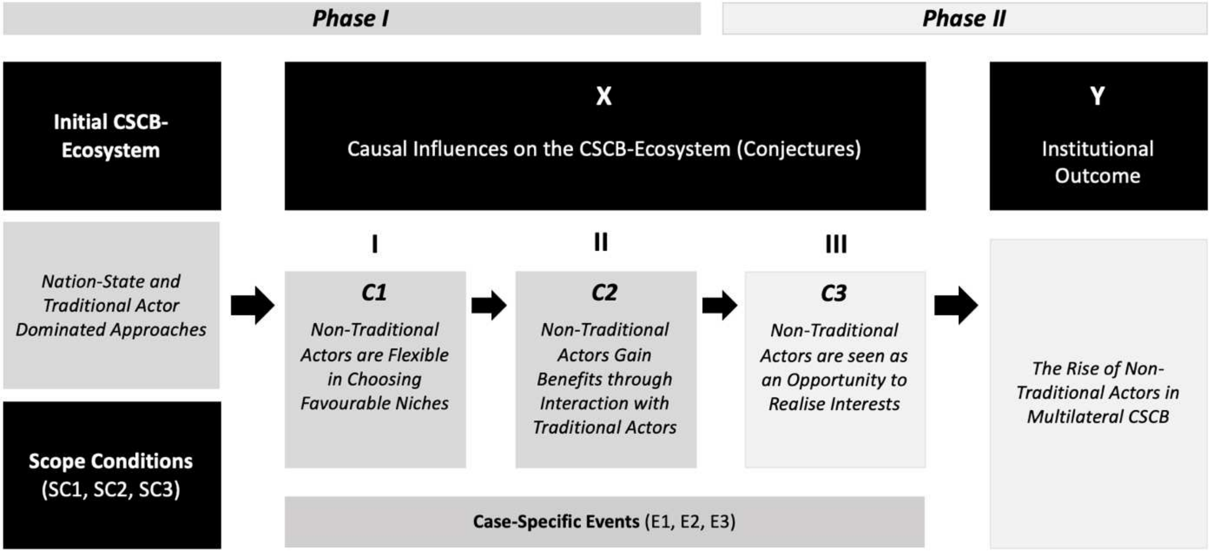
Process Tracing serves as an analytic tool for drawing causal inferences from pieces of evidence based on an in-depth knowledge of the phenomenon in question. It can make decisive contributions to the systematic analysis of political change (Collier, 2011). Explaining-Outcome PT (Beach & Pedersen, 2013) is selected as the iterative strategy for answering the proposed research question. This type of PT (Allison, 1971; Schimmelfennig, 2001; Wood, 2003) relies on an analysis of available evidence, starting with a known outcome and working back to uncover the causal mechanisms producing it (Beach & Pedersen, 2012). A *minimally sufficient* (Beach & Pedersen, 2013) explanation for the rise of NTAs in multilateral CSCB is developed by linking theoretical and case-specific mechanisms. Explaining-Outcome PT enables the application of complementary theories to best explain the outcome by establishing the causal mechanisms that led to it (Checkel, 2005). Following the definition of mechanisms by Wight (2004), they are understood as a “sequence of events and processes (the causal complex) that lead to the event” (Wight, 2004, p. 290). Accordingly, case-specific events can also be defined as mechanisms and support the minimally sufficient explanation.

In Explaining-Outcome PT, the term *causal mechanisms* is employed more broadly than with other variants of PT. The employed strategy to sufficiently explain the outcome is "eclectic theorisation" (Beach & Pedersen, 2013, p. 64). This deductive approach stands for a pragmatic combination of compatible mechanisms into mechanism-conglomerates. Additionally, non-systematic and case-specific parts are added inductively. The possibility to draw references that reach beyond the specific case is ensured by the mechanisms deduced from established theory. Processes can be analysed regarding their chronological and causal structures (Orban & Trampusch, 2019). This research project focuses on tracing parallel causal mechanisms (Elling, 2008), leading to the outcome in question. The strength of the evidence is tested by linking the potential mechanisms to the outcome (Y). Finally, a plausible explanation of multiple X, leading to one Y, is built. Causal inferences are made by testing the sufficiency of the elaborated mechanisms to explain the outcome.

The Process Tracing starts with a deductive approach *(Phase I)*. This approach proceeds similarly to theory-testing PT. Based on existing theorisation, two parallel causal mechanisms – *conjectures* – are deduced. The causal mechanisms are operationalised by translating theoretical predictions to case-specific empirical observations. Causal inferences about the mechanisms are then made based on the empirical data. It is tested whether the deduced mechanisms **(C1, C2)** were present in the case and can explain the outcome (Beach & Pedersen, 2013). These two conjectures are not rivalling but complementary. As the mechanisms **(C1, C2)** provide a substantial yet not minimally sufficient explanation, an additional approach is followed. Informed by the findings of this first phase, another deductive analysis is pursued *(Phase II)*. It explores a separate complementary mechanism, deduced from agency-centred Historical Institutionalism **(C3)**. The process is visualised in **Figure 1**.

Based on the analysis, both theories are deemed insufficient to explain the outcome on their own (Schimmelfennig, 2001). A satisfactory, minimally sufficient explanation is established by the more complex and case-specific combination of both theories. Confirming this as a generalisable theoretical approach for a population of cases isn't the purpose of Explaining-Outcome PT (Beach & Pederson, 2013), nor the aim of this thesis. Instead, an in-depth elaboration on causal influences is provided, a promising foundation for future studies.

Figure 1: Phases I and II of the Explaining-Outcome Process Tracing


Phase I
Phase II
Initial CSCB-Ecosystem
X
Causal Influences on the CSCB-Ecosystem (Conjectures)
Y
Institutional Outcome
Nation-State and Traditional Actor Dominated Approaches
I
C1
Non-Traditional Actors are Flexible in Choosing Favourable Niches
II
C2
Non-Traditional Actors Gain Benefits through Interaction with Traditional Actors
III
C3
Non-Traditional Actors are seen as an Opportunity to Realise Interests
The Rise of Non-Traditional Actors in Multilateral CSCB
Scope Conditions (SC1, SC2, SC3)
Case-Specific Events (E1, E2, E3)

Own visualisation, modified and adapted from Beach & Pedersen (2013)

3.2. Selection of Empirical Data

This thesis draws on different data sources. Most importantly, secondary research literature on CSCB, NTAs, policies, and primary communication by actors. Initially, an overview of dynamics in the international CSCB ecosystem is given. This relies on a structured observation and review of secondary academic and grey literature. The selection of examples for the analysis is based on and guided by this literature review. For the complementary PT, the full range of documents is employed. These documents further include academic publications on CSCB and conference reports. The empirical data was collected using online research and retrieved from publicly accessible sources. The analysis follows a deductive design, complemented by inductive additions and examples based on the retrieved primary and secondary data (see **Annexe 3**).

4. Non-Traditional Actors in Multilateral CSCB

Currently, no commonly agreed-on definition of CBCB exists. This is a logical consequence, considering that both parent concepts, “cybersecurity” and “capacity building”, are contested themselves (Connolly, 2007; Wilén, 2009; Dunn Cavelty & Wenger, 2020). Researchers use the terms “cyber” instead of “cybersecurity” and “capacity development” instead of “capacity building”. This results in at least four different terms for one issue. CSCB is among the most used terms in policy documents (Collett, 2021) and thus selected for this thesis. The preliminary definition this thesis pragmatically works with is proposed by Collett (2021) and builds on Pawlak’s (2014b) earlier definition attempts (see 1.). It has to be pointed out that Collett’s (2021) definition refers to individuals, organisations, and governments. However, *organisations* include, among others, “companies, regional economic communities, international organisations, academia and civil society” (Collett, 2021).[3]

> *“International cybersecurity capacity building is an umbrella concept for all types of activity in which individuals, organisations or governments collaborate across borders to develop capabilities that mitigate risks to the safe, secure and open use of, and relationship with, the digital environment.”*
>
> **Collett (2021, p.8)**

CSCB emerged when the international community agreed that cybersecurity capacities needed international support (Collett & Barmpaliou, 2021). The complex pluralisation of different actors roots in the reconstitution of international affairs due to digital transformation and globalisation (Kulesza & Eggenschwiler, 2020). Today NTAs inhabit core areas of global policy- and decision-making. NTAs have been vital contributors to the evolution and growth of cyberspace itself. This contribution is based on the provision of technological services, soft- or hardware production, and the development of norms (Kulesza & Eggenschwiler, 2020). No country can utilise the full potential of Information and Communication Technologies (ICTs) without fostering CSCB to address the inherent risks. CSCB is key to mitigating negative influences and maximising ICT-related benefits (Hohmann et al., 2017). Actors at all levels, from early adopters in IGOs and governments to NTAs, are a part of ensuring that cyberspace and dependent systems are resilient to attack.

This likewise refers to forerunner states such as Israel, the United Kingdom (UK), the Netherlands, or the United States of America (US), and organisations like the ITU. CSCB includes actors that Risse defines as traditional state actors, namely as “members of the executive, legislature, and judiciary at (supra-)national or subnational levels” (2012, p.8). Simultaneously, CSCB includes actors from academia, such as Oxford University, or multinational companies like Microsoft and Hewlett-Packard (HP). These actors do not just support capacity building. For some, it is a tool for advocating their aims in internet governance, creating access to new markets, or promoting technical standards, short: a (corporate) diplomacy and foreign policy tool (Hohmann et al., 2017).

[3] The definition by Collett (2021) does not employ “multi-stakeholder” or “actor” terms, which this thesis heavily relies on. This, however, is – as noted by Collett – merely due to the more complicated understanding of these terms for non-specialists.

4.1. A Non-Exhaustive Overview of Influential CSCB Actors

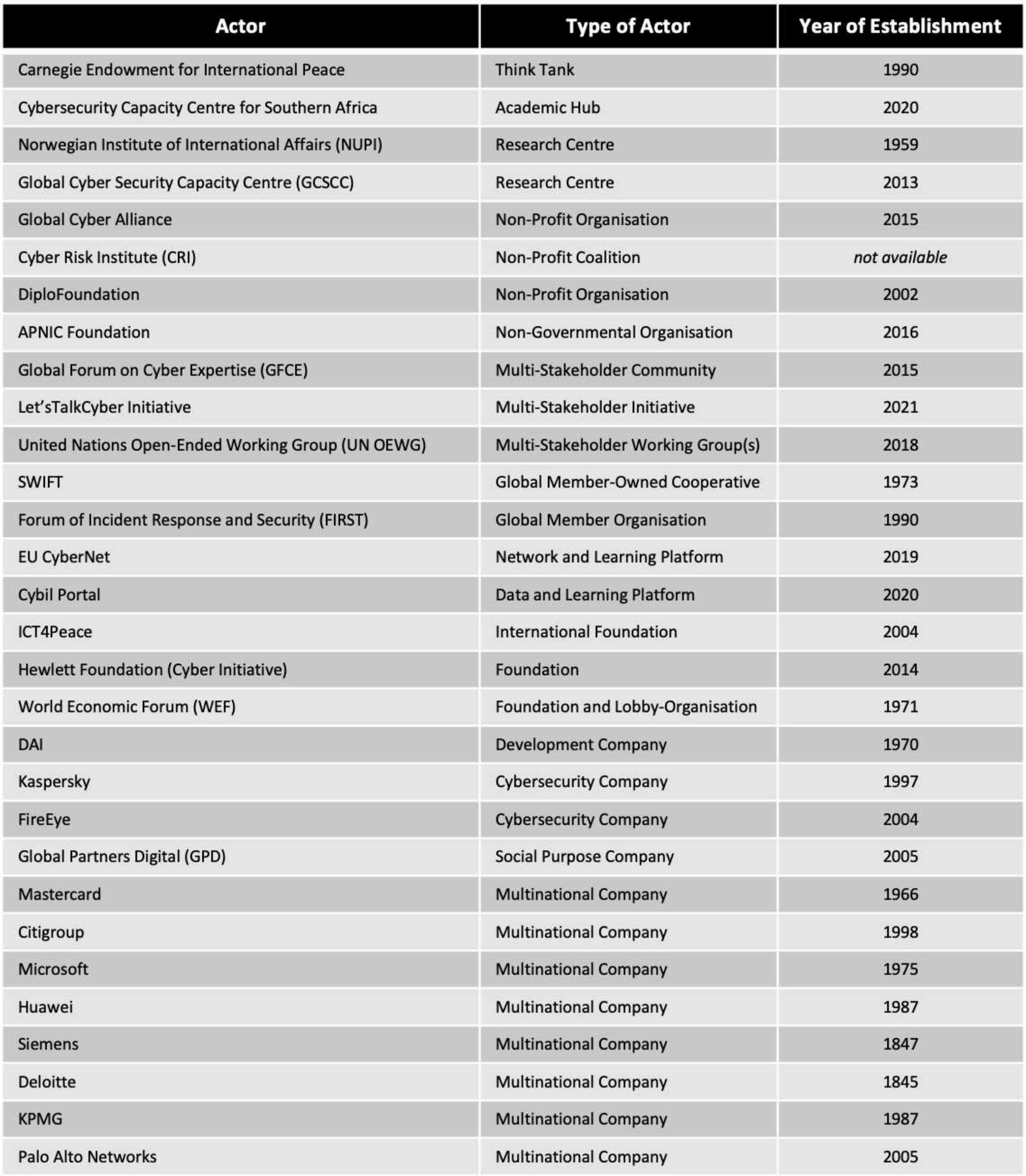
The empirical analysis is based on a careful combination of stakeholder mappings. The original mappings by Carnegie (Maurer & Nelson, 2020), the Cybil Portal (2021b), the Stiftung Neue Verantwortung (Rupp & Herpig, 2021), and the EPRS (2020) are non-exhaustive themselves. The attempted merger and adjustment of the mappings to the sub-field of CSCB explicitly does not claim nor aim to provide an exhaustive overview. It serves as a pragmatic basis for analysing the deduced causal mechanisms by providing a basic overview of some influential traditional (state) actors and non-traditional actors. What is intriguing about actors and communities in the CSCB ecosystem? Undoubtedly how the "niche" character of cybersecurity in international affairs and the national security link of the issue area influence its composition (Collett & Barmpaliou, 2021).

The Cybil Portal (2021b), for instance, differentiates policymakers, governments, International Organisations (IOs), civil society, knowledge institutions and the private sector. While there is a total of 71 listed IGOs, non-traditional actors comprise the private sector (135), knowledge institutions (106) and civil society (112) Cybil Portal (2021b). The (non-traditional) private sector alone comprises various sub-types of actors.[4] Traditional actors in CSCB, on the other hand, include – but are by no means limited to – the International Monetary Fund (IMF), the World Bank Group (WBG), the United Nations Group of Governmental Experts (UN GGE)[5], the United Nations Institute for Disarmament Research (UNIDIR), the United Nations Office for Disarmament Affairs (UNODA), the United Nations Office on Drugs and Crime (UNODC), the Organisation for Security and Co-operation in Europe (OSCE), the Council of Europe (CoE), Europol, Interpol, the International Telecommunication Union (ITU), the North Atlantic Treaty Organisation (NATO) and regional organisations (Association of Southeast Asian Nations (ASEAN), African Union (AU), Organisation of American States (OAS), European Union (EU).

[4] Non-traditional private sector actors in CSCB include: ICT Companies (e.g., Microsoft, Hewlett Packard), Service Companies (e.g. Deloitte, KPMG), Cybersecurity Companies (e.g., FireEye, Kaspersky), Telecoms Companies (e.g., Huawei), Financial Sector Actors (e.g., Mastercard, SWIFT), and Project Companies (e.g., small and medium-sized enterprises) (Collett & Barmpaliou, 2021).

[5] The UN GGE consists of just 25 national experts. The UN OEWG, on the other hand, is open to all states. The UN OEWG's mandate also covers a broader range of issues (Collett, 2021).

Figure 2: **Non-Exhaustive Mapping of Influential NTAs in International CSCB**



Actor	Type of Actor	Year of Establishment
Carnegie Endowment for International Peace	Think Tank	1990
Cybersecurity Capacity Centre for Southern Africa	Academic Hub	2020
Norwegian Institute of International Affairs (NUPI)	Research Centre	1959
Global Cyber Security Capacity Centre (GCSCC)	Research Centre	2013
Global Cyber Alliance	Non-Profit Organisation	2015
Cyber Risk Institute (CRI)	Non-Profit Coalition	*not available*
DiploFoundation	Non-Profit Organisation	2002
APNIC Foundation	Non-Governmental Organisation	2016
Global Forum on Cyber Expertise (GFCE)	Multi-Stakeholder Community	2015
Let’sTalkCyber Initiative	Multi-Stakeholder Initiative	2021
United Nations Open-Ended Working Group (UN OEWG)	Multi-Stakeholder Working Group(s)	2018
SWIFT	Global Member-Owned Cooperative	1973
Forum of Incident Response and Security (FIRST)	Global Member Organisation	1990
EU CyberNet	Network and Learning Platform	2019
Cybil Portal	Data and Learning Platform	2020
ICT4Peace	International Foundation	2004
Hewlett Foundation (Cyber Initiative)	Foundation	2014
World Economic Forum (WEF)	Foundation and Lobby-Organisation	1971
DAI	Development Company	1970
Kaspersky	Cybersecurity Company	1997
FireEye	Cybersecurity Company	2004
Global Partners Digital (GPD)	Social Purpose Company	2005
Mastercard	Multinational Company	1966
Citigroup	Multinational Company	1998
Microsoft	Multinational Company	1975
Huawei	Multinational Company	1987
Siemens	Multinational Company	1847
Deloitte	Multinational Company	1845
KPMG	Multinational Company	1987
Palo Alto Networks	Multinational Company	2005

Own visualisation adapted from Maurer & Nelson (2020), Cybil Portal (2021b), Rupp & Herpig (2021) and EPRS (2020)

4.2. The Changing Face of Multilateralism

“It is a vibrant and diverse biotope that is benefitting from its interdisciplinarity, its relevance for policy, and its cognisance of the interplay between technological possibilities and political choices.”

Dunn Cavelty & Wenger (2019)

The number of involved actors in public and private sectors continues to grow in global governance (Seyle, Weiss, & Coolidge, 2013).[6] What is interesting about this dynamic is the

[6] See the attached **Annexe 2** for a visualisation of this trend.

irregular distribution among the types of these organisations. IGOs attain a natural limit (Abbott et al., 2016). This does not account for their networks, financial resources and initiatives. These have increased. However, the significant share of the increase in actors can be attributed to non-traditional actors (Seyle et al., 2013).

The recently (23 September 2021) published European Institute for Security Studies (EUISS) report on International Cyber Capacity Building: Global Trends and Scenarios (Collett & Barmpaliou, 2021) identifies four major trends in CSCB. The research question can be situated between trends one and three. Trend 1 (*The field of Cybersecurity Capacity Building is growing*) is relevant to acknowledge as it stresses how rapidly the number of involved actors in CSCB increases (Collett & Barmpaliou, 2021). The growing CSCB ecosystem of international cooperation is constantly defining its boundaries and structures (Collett & Barmpaliou, 2021). Trend 3 (*More Communities of Practice are using C(S)CB to pursue their aims*) highlights the practical relevance of the research question. It outlines how actors pursue different aims and employ a range of approaches (Collett & Barmpaliou, 2021). The CSCB ecosystem mirrors this architecture of loosely interconnected communities. The role of NTAs in CSCB has grown in investment volume, size, and relevance (Collett & Barmpaliou, 2021). Acknowledging this is crucial, as new actors eventually tackle common cybersecurity challenges while pursuing individual ambitions (Collett & Barmpaliou, 2021).

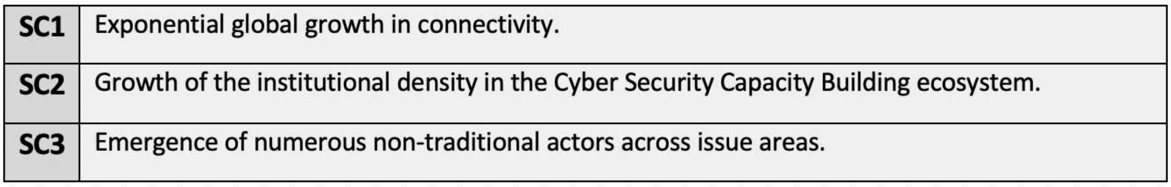
> *"Companies are creating new not-for-profit organisations, forming alliances and consortia, launching cyber training academies, financing CCB projects directly or through their foundations, convening strategic events, presenting proposals and taking an active role in platforms."*
>
> **Collett & Barmpaliou (2021, p. 45)**

NTAs obtain heterogeneous roles. Some implement funded projects, others finance these. Some provide pro-bono services, others engage at the front line. Some provide coordination, others even contribute to international policy negotiations. Several NTAs work towards CSCB by providing cybersecurity training and fostering public-private tech hubs (Collett & Barmpaliou, 2021). The most prominent example of a highly influential non-traditional organisation in the CSCB ecosystem is the Global Forum on Cyber Expertise (GFCE) (Collett & Barmpaliou, 2021, p. 45). This thesis is titled *Multilateral Approaches to Cyber Security Capacity Building: The Rise of Non-Traditional Actors*. Giving a clear idea of how *multilateral* is understood as a concept is respectively vital. 20th-century multilateralism can be characterised as “hegemonic, value-based, and revolv(ing) around states” (Kortunov, 2020). Today, however, this conceptualisation is outdated. Instead, another trend can be observed. It is a shift towards a “project-based multilateralism that is inclusive to non-state actors, with shared values as a goal, not a precondition” (Kortunov, 2020). Rittberger (2008) underlines this by reemphasising how the broad range of institutional arrangements can no longer be attributed to executive intergovernmental multilateralism. Contrary to the former exclusive concept of “executive multilateralism in intergovernmental organisations” (Rittberger, 2008, p.3), increasing space and influence for NTAs points towards a more inclusive “institutionalisation of global regulatory or (re-)distributive policy-making” (Rittberger, 2008, p.2). These “inclusive, multipartite institutions of global governance” (Rittberger, 2008, p.2) do not just allow traditional (state/ inter-state) actors but also NTAs as members. This includes their access to decision-making processes in policy-making. The new, more inclusive governance is also referred to as “heterarchy” instead of the former “regulated anarchy” (Rittberger, 2008, p. 15).[7]

5. Empirical Analysis

The qualitative empirical analysis is designed to find answers to the research question *(How can the rise of non-traditional actors in the multilateral Cyber Security Capacity Building ecosystem be explained?)*. The aim is to collect sufficient evidence to establish the causal mechanisms resulting in the institutional outcome (see **Figure 1**). Each deduced conjecture **(C1, C2, C3)** comprises a parallel process step. The outcome of each conjecture thus is also the final outcome in question, namely the rise of NTAs in multilateral CSCB. This conceptualisation is based on the understanding that parallel rather than chronologically aligned mechanisms constitute the process. Accordingly, **C1** and **C2** are examined in their causal relevance in the first phase *(Phase I)* of the research. After evaluating their combined explanatory power, **C3** is added in a second phase *(Phase II)*.

Figure 3: Scope Conditions



SC1	Exponential global growth in connectivity.
SC2	Growth of the institutional density in the Cyber Security Capacity Building ecosystem.
SC3	Emergence of numerous non-traditional actors across issue areas.

[7] According to Rittberger, *heterarchy* describes „an increasingly dense network of institutions of global governance, created and maintained by public and private actors […] through horizontal policy coordination and cooperation where different groups of actors (states, intergovernmental organisations, civil society organisations, […] private sector actors) are sensitive to each other’s values and interests and dependent on one another to achieve collective goals“ (2008, p.16).

All conjectures are based on three scope conditions **(SC1, SC2, SC3)** derived from an overview of current research on the CSCB environment. The first scope condition **(SC1)** is the exponential global growth in connectivity (Hohmann et al., 2017, p. 6). Scope condition 2 **(SC2)** is the growth of the institutional density in CSCB. It is related to OE theory, where legitimation and competition are identified as two processes that explain the rise or failure of organisational forms. Both are based on density, as structural variable (Abbott et al., 2016). Taking **Annexe 2** into account, it is apparent that the number of NTAs rises rapidly compared to traditional IGOs. Additionally, lots of them have emerged across different issue areas within recent years, including climate, health, and cybersecurity. This remarkable emergence is considered as the third scope condition **(SC3)** for the process.

The operationalisation attributes expected observations and measuring to each of the three causal mechanisms **(C1, C2, C3)**. The used model is based on the operationalisation guidelines delineated by Beach and Pedersen (2013). The attribution of expected observations is conceptualised by merging theoretical implications and thorough knowledge of the specific ecosystem. Measuring is set to be conducted by a qualitative examination of evidence.

5.1. Causal Effects Based on Organisational Ecology Theory

The conjectures one and two **(C1, C2)** are derived from (Abbott et al., 2016) and have been swiftly adapted to the processes in the CSCB ecosystem and NTAs. Abbott et al. (2016) propose one additional conjecture for the field of climate governance. This conjecture, focusing on lower entry costs for NTAs, is disregarded for this approach. This is due to both theoretical and practical reasons. Theoretically, the factor of lower entry costs is deemed less pivotal in CSCB due to the widespread public access to the internet. Practically, the observations this conjecture would come with are hardly measurable in the young and dynamic CSCB field, given the non-exhaustive mappings and the chosen qualitative approach. Instead, this thesis takes on Abbott et al.'s (2016) recommendation by including an agency-centred, HI-approach for a more holistic understanding of ecosystem changes. Accordingly, the third conjecture **(C3)** is based on DiMaggio (1988), as recited by (Emmenegger, 2021).

As mentioned earlier, each conjecture is connected to observable implications. These include both structural and intrinsic characteristics of organisational forms and their environments that impact actors (Abbott et al., 2016). The operationalisation is outlined in the following tables **(Figure 4, Figure 5, Figure 7)**. This research is designed in accordance with the Explaining-Outcome PT principles established by Beach and Pedersen (2013). Each conjecture is operationalised by defining the needed evidence for the different types of tests. It is thereby recognised that there are different types of evidence regarding their relative necessity for establishing causal mechanisms (Bennett & Checkel, 2014; Collier, 2011; Mahoney, 2012; Rohlfing, 2014). This thesis follows the suggestion of (Ricks & Liu, 2018) and differentiates four types of tests *(Straw-in-the-Wind, Hoops, Smoking-Gun, Doubly-Decisive)*. In accordance with the research question, Hoops and Smoking-Gun Tests are considered the most important for the chosen approach. Nonetheless, Straw-in-the-Wind Tests are carefully conducted as they help to strengthen the conjectures. To better understand the general approach, these tests are outlined in detail for the initial analysis of **C1** and then applied for the following conjectures **(C2, C3)** accordingly.

5.1.1. Conjecture 1

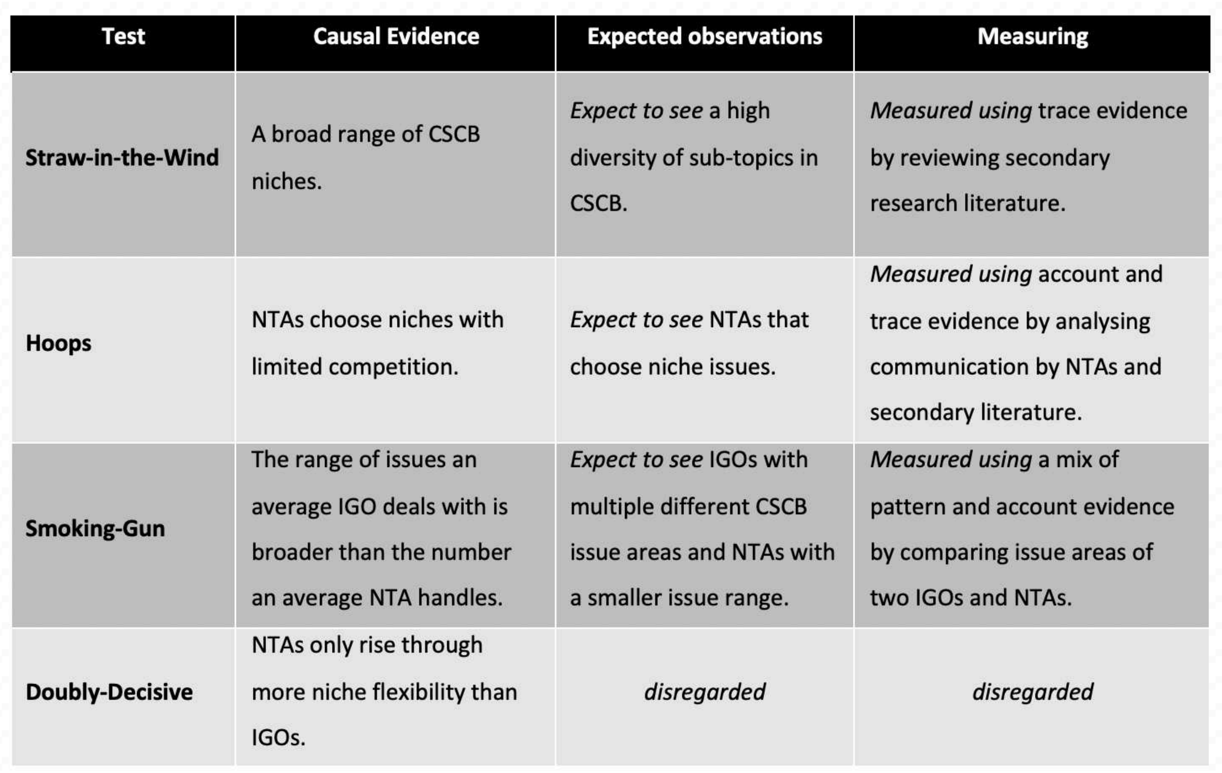
C1	**When non-traditional actors are flexible in choosing favourable niches, *it results in the rise of non-traditional actors in multilateral Cyber Security Capacity Building.***

C1 is deduced from the OE framework. It states that when NTAs are flexible in choosing favourable niches (IV), it results in the rise of NTAs in multilateral CSCB (DV). The operationalisation of this first conjecture is outlined in **Figure 4**.

First, evidence for the weakest test, the **Straw-in-the-Wind Test**, is examined. This test can increase the plausibility of the conjecture but is neither a necessary nor a sufficient test for accepting or rejecting the premise. The primary causal evidence is the empirical existence of a broad range of CSCB niches. The expected observation is a high diversity of sub-topics in CSCB. This is measured by reviewing secondary research literature. Particularly in CSCB, *capacity* refers to a broad range of issue areas. It includes a variety of projects of the different (non-)traditional actors. A common aim can somewhat be located between building a consensus on cybersecurity by strengthening information flows and international cooperation (Calandro & Berglund, 2019). Methods and shapes for achieving it, however, are multifaceted. They range from law enforcement capacities and policy drafting to public awareness campaigns. Another attempt at structuring the different sub-topics of CSCB is the definition of three overarching dimensions by Pawlak & Barmpaliou (2017).

Figure 4: Operationalisation of Conjecture 1 (C1)

C1: When non-traditional actors are flexible in choosing favourable niches, *it results in the rise of non-traditional actors in multilateral Cyber Security Capacity Building.*



Test	Causal Evidence	Expected observations	Measuring
Straw-in-the-Wind	A broad range of CSCB niches.	*Expect to see* a high diversity of sub-topics in CSCB.	*Measured using* trace evidence by reviewing secondary research literature.
Hoops	NTAs choose niches with limited competition.	*Expect to see* NTAs that choose niche issues.	*Measured using* account and trace evidence by analysing communication by NTAs and secondary literature.
Smoking-Gun	The range of issues an average IGO deals with is broader than the number an average NTA handles.	*Expect to see* IGOs with multiple different CSCB issue areas and NTAs with a smaller issue range.	*Measured using* a mix of pattern and account evidence by comparing issue areas of two IGOs and NTAs.
Doubly-Decisive	NTAs only rise through more niche flexibility than IGOs.	*disregarded*	*disregarded*

Own visualisation, modified and adapted from Beach & Pedersen (2013)

Pawlak and Barmpaliou (2017) distinguish between the development of individual capacities, the design of institutional frameworks, and the strengthening of efficient organisational structures. Each of these dimensions includes multiple sub-topics. The development of individual capacities alone, for instance, refers to CSCB measures directed at improving skills, competence, attitudes, and knowledge (Pawlak & Barmpaliou, 2017). The Cybil Portal (2021b) clusters CSCB activities in four main themes. These range from Cyber Incident Management & Critical Information Protection, Cyber Security Culture & Skills, Cyber Security Policy & Strategy, and Cyber Security Standards to Cybercrime (Cybil Portal, 2021b). Each of these themes further incorporates around 2-3 sub-topics. While this successful Straw-in-the-Wind test is not sufficient for confirming the conjecture, it certainly provides a valuable benchmark (Collier, 2011). This initial assessment can finally help to add up to important evidence that affirms **C1**. Given the context, this is the first piece of solid trace evidence.

Based on this initial success, a **Hoop Test** is conducted. If the conjecture fails to pass this test, **C1** can be falsified. Passing this test, however, doesn't automatically validate it. It just further strengthens the premise. In the case for **C1**, stating that NTAs are flexible in choosing favourable niches, NTAs must actually select these. The expected observation is to see NTAs that focus on specific issues. This is measured by analysing related communication by NTAs. Flexibility, a structural feature, is understood as one of the intrinsic characteristics of organisational forms (Abbott et al., 2016), influencing the relevant ecosystem. Flexibility is deemed to affect the individual actors (Abbott et al., 2016). This focus on specific issues is enhanced by the last United Nations Open-Ended Working Group (UN OEWG) report (Collett, 2021, p. 12). The concurrent appeal is that "specific activities should have a clear purpose and be results-focused while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment" (UN OEWG, 2021, p. 8). This shows that the focus on specific issues can – and should – still be advanced from its current state. UN OEWG-proposed Cyber Security Capacity Building principles include tailoring CSCB initiatives to the many circumstances and requirements. While all actors should participate actively, their responsibilities should be particular.

Examples include the evaluation of CSCB-activities, the execution, monitoring, and design tasks (Collett, 2021, p. 12). Multiple CSCB actors already show such a specific approach. Smaller cyber companies, for instance, tend to have particular expertise in implementing competitive international CSCB projects. While they often evolve in one country, they successfully combine international development and cybersecurity skillsets on the international level (Collett & Barmpaliou, 2021). This is a remarkable trend in states with evolving environments of consultants, academics and small-scale CSCB companies (Collett & Barmpaliou, 2021). A strong issue-specific niche for NTAs is the coordination of CSCB actors and their initiatives. This roots in rising concerns about inefficient duplication and gradual fragmentation of activities in the CSCB ecosystem (Eggenschwiler, 2018). The most renowned NTA that arose from this vision in 2015 is the GFCE. It was established as a hub for CSCB-coordination, precisely for knowledge-sharing, best-practice exchanges and initiative creation. Guided by an advisory board of NGOs, academia and technical stakeholders, it has since been open for IGOs, nation-states, and private companies alike (Eggenschwiler, 2020). As another NTA example, Global Partners Digital (GPD) focuses on the niche of fighting disinformation from a human rights perspective (GPD, 2020). The Global Cyber Alliance's CSCB programme *(Capacity & Resilience)* strictly focuses on enabling growth by building cyber risk capacities. Related projects focus on a cybersecurity toolkit and a flipbook (Global Cyber Alliance, 2021). The Cyber Risk Institute (CRI) is an example of NTAs focusing on stakeholders within a concise field. The CRI is a non-profit coalition of actors in the financial services sector. The institute aims to advance cybersecurity through standardisation by providing a specific "Cyber Profile Tool" for a cybersecurity assessment (CRI, 2021). On the other hand, actors who already work issue-specific start including CSCB in their work (Pawlak & Barmpaliou, 2017). **C1,** therewith passes this second, more demanding test. The existence of the necessary criterion (Collier, 2011) is established. While **C1** thus remains under consideration, this does not mean that it is verified.

The next test is the **Smoking-Gun Test**. Passing this test does not provide a necessary but a sufficient criterion for accepting the causal mechanism. The causal evidence for this test is defined as: the range of issues an average IGO deals with is broader than the number an average NTA handles. This evidence comes with the expected observation of IGOs with a wide range of CSCB issue areas and NTAs with a minor issue range. It is tested using a mix of pattern and account evidence by comparing issue areas of two typical IGOs and two NTAs. The wide range of CSCB issues comes with less functional specificity of traditional organisations, as it fosters complex and multi-purpose structures. Traditional multilateral meetings turn into "loose platforms" for exchange on policy-making or superficial discussions of opinions (Rüland, 2018, p. 10). The *trans-sovereign problems* (Rittberger, 2008, p. 6) connected to CSCB exceed the capacities of traditional international IGOs.[8] This is because actors responsible for and affected by those issues are non-traditional, "transnationally active private entities" (Rittberger, 2008, p. 6). Traditional actors, particularly IGOs, seek to demonstrate how they fulfil their extensive mandates. This presents an incentive to pursue activities in an ever-broader conglomerate of issue areas (Abbott et al., 2016) to respond to challenges and opportunities. In addition, state vetoes and oversight make the creation of new emanations more attractive than the formation of new IGOs (Abbott et al., 2016). NTAs, on the contrary, have a strong incentive to limit competition. This is due to their resource scarcity and endangerment of survival (Abbott et al., 2016). NTAs more flexibly occupy areas less restricted by oversight and not as crowded.

[8] Examples that Rittberger (2008) names for *transsovereign problems* are global pandemics, environmental threats and terrorism.

A few examples of this are explored. First, by zooming in on a sub-type of NTAs: multinational cybersecurity companies. HP, for instance, names just three explicit goals for the Hewlett Foundation's activities in CSCB.

> **(1)** "*Build a set of core institutions with sufficient depth of expertise to deliver solutions that take competing values and trade-offs to pressing cyber policy challenges seriously.*"
> **(2)** *"Create a talent pipeline to produce experts with the necessary mix of technical and non-technical skills and knowledge to staff these and other institutions, including government and industry."*
> **(3)** *"Support the development of infrastructure to translate and disseminate the work of these institutions that can be understood and used by decision-makers and the public."*
>
> **Hewlett Foundation (2021)**

The Palo Alto Networks Cybersecurity Academy, another CSCB-NTA, explicitly focuses on skills development by creating degree programmes with entry-level to intermediate classes and hands-on practices free of charge for educational institutions (Collett & Barmpaliou, 2021, p. 46). The ITU and the European Union Agency for Cybersecurity (ENISA) are selected for the contrastive look at traditional actors. The ITU covers themes from an extremely vast array. They range from Cyber Security Strategies, National Assessments, Cybercrime Training and Prevention to Cyber Security Standards (Cybil Portal, 2021a). Their initiatives in the "Cybersecurity" priority area alone include a "Women in Cyber Mentorship Programme", a "Guide to Developing a National Cybersecurity Strategy", and "Global Cyber Drill"-events, as well as "Cyber Online Protection"-materials (ITU, 2021c). "Capacity development" is defined as a separate neighbouring domain and comprises projects like "Digital Transformation Centres" and "Digital Skills Assessment Guidebook" (ITU, 2021b). Most significantly, these areas are just two out of ten priorities that the ITU defines for its engagement. This underlines how much broader the range of CSCB issues that an average IGO deals with is compared to NTAs. ENISA pursues its CSCB activities under the mandate of Regulation (EU) 2019/881 and Regulation (EU) No 526/2013 (ENISA, 2021). The activities of ENISA are clustered into seven sub-areas, with explicit capacity building as just one of them. Those findings certainly strengthen **C1**. This third test is, however, is also somewhat weakened by additional empirical evidence. This regards highly established NTAs such as the GFCE and ICT4Peace. These NTAs continue to broaden their CSCB-related activity areas "across a range of critical domains" (ICT4Peace, 2016). ICT4Peace, for instance, elaborates on the width of their activity areas, claiming that their complex and sensitive work "range(s) from leveraging technology to counter violent extremism at the local level to addressing threats to cyberspace at the global level" (Stauffacher, 2021, p. 1). This implies that a broader range of CSCB issues can also be observed among the most established multi-stakeholder NTAs. This, however, strictly does not regard the majority of NTAs. Thus, **C1** is only slightly weakened and passes this critical test.

The cumulative evidence provides strong support for the claim that the flexibility of non-traditional actors to choose favourable domains is a causal mechanism leading to the rise of NTAs in multilateral CSCB. Finally, passing the **Doubly Decisive Test** would require empirical proof that *only* the claim made with **C1** can be supported, namely, that it is only the flexibility of NTAs to choose favourable niches leading to the rise of NTAs in multilateral CSCB. The purpose of this PT test would be to eliminate any other possible explanations (conjectures) for the outcome. It is thus less reasonable for the aim to find a minimally sufficient explanation for the outcome by combining and not contrasting causal mechanisms.[9] Considering the evidence from the three other tests, there – nonetheless – is strong support for **C1**.

5.1.2. Conjecture 2

C2	**When non-traditional actors gain benefits through interaction with traditional actors, *it results in the rise of non-traditional actors in multilateral Cyber Security Capacity Building.***

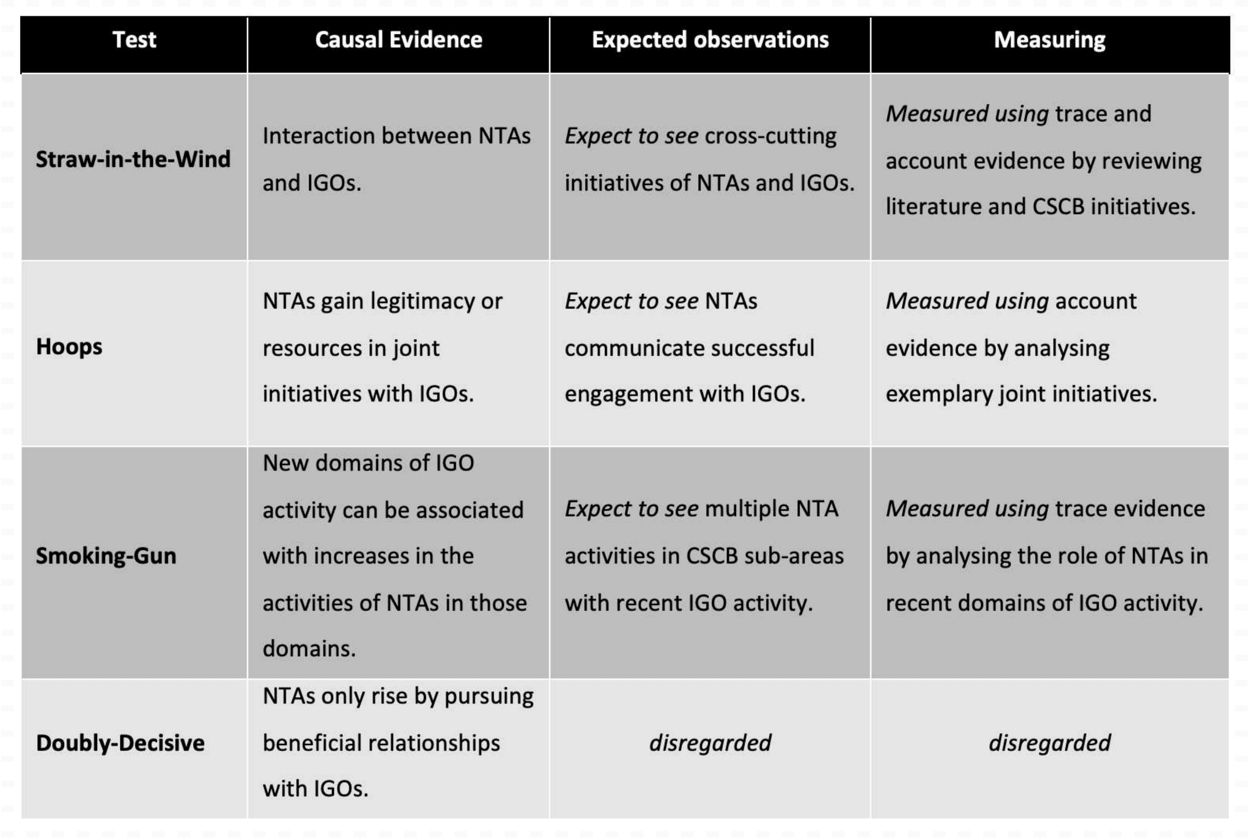
Like **C1**, **C2** is derived from the OE framework. It claims that when non-traditional actors gain benefits through interaction with traditional actors (IV), it results in the rise of NTAs in multilateral CSCB (DV). The operationalisation of this second conjecture (C2) is outlined in **Figure 5**.

The needed causal evidence for an initial **Straw-in-the-Wind Test** is an empirically apparent interaction between NTAs and traditional actors, such as IGOs. The expected observation is cross-cutting initiatives of NTAs and IGOs. The flexible character of NTAs (see **C1**) also advances their ability to form complementary relationships (Abbott et al., 2016). What actors collaborate within capacity-building initiatives is highly relevant for their success (Pawlak, 2014b). This is due to the root causes for participating in specific initiatives. These are to be located in resource distribution, access to decision-making, trust and ultimately a similar aim (Pawlak, 2014b). "Therefore, a decision about whom to cooperate with and to what extent is a strategic one and has an impact" (Pawlak, 2014b, p. 61).

[9] This logic is also applied for the other conjectures (C2, C3) but will no longer be elaborated on specifically.

Figure 5: Operationalisation of Conjecture 2 (C2)

C2: When non-traditional actors gain benefits through interaction with traditional actors, *it results in the rise of non-traditional actors in multilateral Cyber Security Capacity Building.*



Test	Causal Evidence	Expected observations	Measuring
Straw-in-the-Wind	Interaction between NTAs and IGOs.	*Expect to see* cross-cutting initiatives of NTAs and IGOs.	*Measured using* trace and account evidence by reviewing literature and CSCB initiatives.
Hoops	NTAs gain legitimacy or resources in joint initiatives with IGOs.	*Expect to see* NTAs communicate successful engagement with IGOs.	*Measured using* account evidence by analysing exemplary joint initiatives.
Smoking-Gun	New domains of IGO activity can be associated with increases in the activities of NTAs in those domains.	*Expect to see* multiple NTA activities in CSCB sub-areas with recent IGO activity.	*Measured using* trace evidence by analysing the role of NTAs in recent domains of IGO activity.
Doubly-Decisive	NTAs only rise by pursuing beneficial relationships with IGOs.	*disregarded*	*disregarded*

Own visualisation, modified and adapted from Beach & Pedersen (2013)

The increasing interdependencies between non-traditional and traditional CSCB actors create incentives for “multipartite cooperation” (Rittberger, 2008, p. 19). Next to energising effects and more inclusive outcomes, acquiring new resources is a significant incentive for this cross-cutting diversification of initiatives. Resources may be authority and legitimacy, funding, or more experienced expertise. In the current CSCB environment, these resources often remain spread across many different actors (Pawlak, 2014b). An example of such cooperation in CSCB is the Commonwealth Cyber Declaration Programme developed after the 2018 Commonwealth Cyber Declaration. In this programme, Citigroup partnered with Microsoft, the UK government and Templar Executives with the common aim to train more than 1000 individuals across the entire Commonwealth (Maurer & Nelson, 2020).[10] The feedback on this project was very positive, as all the actors could contribute their specific knowledge. The UK Foreign, Commonwealth & Development Office described the contribution of Citigroup as a valuable “training and information gathering support” (Maurer & Nelson, 2020, p. 131). The

[10] Templar Executives is a cybersecurity consultancy.

Forum of Incident Response and Security Teams (FIRST) is another excellent example, bringing together a "wide variety of security […] teams including product security teams from the government, commercial, and academic sectors" (FIRST, 2021). Let'sTalkCyber, for instance, is sponsored by the Australian Government, Global Affairs Canada, EU Cyber Direct, GPD, and Microsoft (Let'sTalkCyber, 2021). With dual responsibility for technical and financial assistance for CSCB activities, the World Bank relies both on its experts and external cooperation partners. A further example is the 2016 Digital Development Partnership (DDP) (Pawlak & Barmpaliou, 2017). The GFCE, as a final instance, has 42 founding members: six IGOs, seven private-sector actors, and 29 states (CFR, 2015). As apparent with these numerous instances, **C2** passes this test and is strengthened in its informative value.

The evidence for the **Hoops Test** is defined as NTAs gaining legitimacy or resources in joint initiatives with IGOs. This is expected to be observable by reviewing related communication by NTAs. Non-traditional actors are keen to strengthen relationships with traditional actors (Collett & Barmpaliou, 2021, p. 47). As such joint initiatives promise opportunities, an effort to create cross-cutting alliances can be observed (Collett & Barmpaliou, 2021). Among the most prominent examples for related NTA engagement and communication is the multinational company Microsoft. Microsoft has not just played a crucial part in both the Paris Call for Trust and Security in Cyberspace and the Cybersecurity Tech Accord alliances (Collett & Barmpaliou, 2021). Furthermore, Microsoft actively communicates successful collaboration. This includes blog publications on "Partnering with governments to help protect democracy", claiming that Microsoft's "partnerships help provide security and privacy for governments, campaigns, and democratic processes" (Microsoft, 2021). The most current example is Microsoft's statement on their role in launching the European Cyber Agora 2021 (Rozentāle, 2021). As a multi-stakeholder platform, the Cyber Agora is designed to bridge the gap between non-traditional and traditional actors by promoting collaboration and evidence-based cybersecurity policy-making (Lété, 2021). Quite similarly, the GFCE communicates its contribution to the Cyber Security Initiative in OAS member states, pointing out how this "recognises the importance of having a comprehensive approach" (GFCE, 2018). This test further strengthens **C2**.

The association of new domains of IGO CSCB activity with an increase of the activities of non-traditional actors in those domains is regarded as strong causal evidence for a **Smoking-Gun Test**. It is expected to see multiple NTA activities in CSCB sub-areas with recent IGO activity. CSCB gradually spread throughout the agendas of traditional actors like the EU, the World Bank, the AU, ASEAN, the OAS and the ITU (Pawlak & Barmpaliou, 2017). Pursuing complementary or even parallel activities to respective IGO policies and programmes is a legitimation strategy of NTAs (Abbott et al., 2016). This complements Pawlak's framework for perceiving CSCB as a foreign relations instrument (Pawlak, 2016a). As this understanding can also be extended beyond traditional actors, it sheds light on the aims and activities of NTAs. NTAs accordingly set technical standards and build infrastructures that strengthen the ability of traditional (state) actors to perform their cybersecurity functions (Calandro & Berglund, 2019). CSCB projects like Microsoft's cloud computing engagement, Huawei's 5G rollout (Calandro & Berglund, 2019), or Siemens' Charter of Trust (Eggenschwiler, 2019) are non-traditional programmes built on earlier IGO engagement, yet with their own long-term priorities. An explicit statement is made by the Hewlett Foundation, reiterating its mission as a neutral, non-profit player (Hewlett-Foundation, 2021). Most importantly, they clearly outline how they build on the activities of IGOs:

> *"We are not responsible for responding to the myriad latest threats and challenges that government and industry must triage each day. We are explicitly agnostic as to specific policy outcomes, seeking only to build a field that can generate robust debate and analysis in order to stimulate better and more strategic cyber policies."*
>
> **Hewlett Foundation (2021)**

Finally, it can easily be observed that many CSCB initiatives continue to be launched in ever-new areas. These efforts, however, are at risk to duplicate each other due to lacking strategy (Hameed et al., 2018). Looking at the sum of evidence for these tests, **C2** is sufficiently established as another parallel, relevant mechanism for the rise of NTAs in multilateral CSCB.

5.1.3. Evaluation and Case-Specific Events

Considering the collected evidence from these two conjectures, it can be concluded that OE mechanisms provide substantial insights. These insights regard causal influences of both the niche-flexibility of NTAs **(C1)** and the beneficial interaction with traditional actors **(C2)**. However, without denying their existence, these two conjectures cannot account for certain turning points. Sudden accelerations in the number of NTAs and their initiatives can hardly be explained. This is also true for traditional actors' inherent disposition – agency – to engage with non-traditional actors, which can scarcely be explained sufficiently without taking agency into account.

First, drawing on the new insights of this analysis *(Phase I)*, the **failure of the 2016/2017 United Nations Group of Governmental Experts (UN GGE)** is inductively added as a case-specific event **(E1)** of causal importance for the institutional outcome (the rise of NTAs in multilateral CSCB).[11] The UN GGE did not include any provisions for non-traditional participation. The collapse of the 2016-2017 UN GGE was finally due to the inability to find any consensus for a report. Subsequently, **cybersecurity incidents of international extent** occurred **(E2)**, prominently the WannaCry and Petya/NotPetya incidents.[12] This led to a "noticeable surge" (Kulesza & Eggenschwiler, 2020, p. 248) in the number of non-state initiatives aiming at CSCB. It also put the routine of discussions in the First Committee of the General Assembly under pressure (Delerue & Korzak, 2020). Based on this **(E1, E2)**, the **United Nations Open-Ended Working Groups (UN OEWG) decision to include NTAs** has to be added as another case-specific event of causal importance for the rise of NTAs **(E3)**. The increasing levels of influence and interest by non-traditional participants illustrated the rising pressure to enable non-traditional, multi-stakeholder participation in the UN debate (Delerue & Korzak, 2020; Let'sTalkCyber, 2021). Thus, two parallel UN processes were established in 2018. On the one hand, another GGE group, and on the other hand, the UN OEWG (Delerue & Korzak, 2020).

> *"The novelty of the intersessional multi-stakeholder meeting was matched by its success: 113 non-state organisations registered to take part, including private companies, NGOs, and universities from all regions of the world."*
>
> **Delerue & Korzak (2020)**

The UN OEWG was designed to include an "intersessional consultative meeting" (Delerue & Korzak, 2020). This inclusive UN OEWG therewith marks a significant turning point, as such intersessional consultation with non-traditional stakeholders has since been praised by non-traditional and traditional (state) actors alike (Let'sTalkCyber, 2021).[13] Including **E1**, **E2**, and **E3**

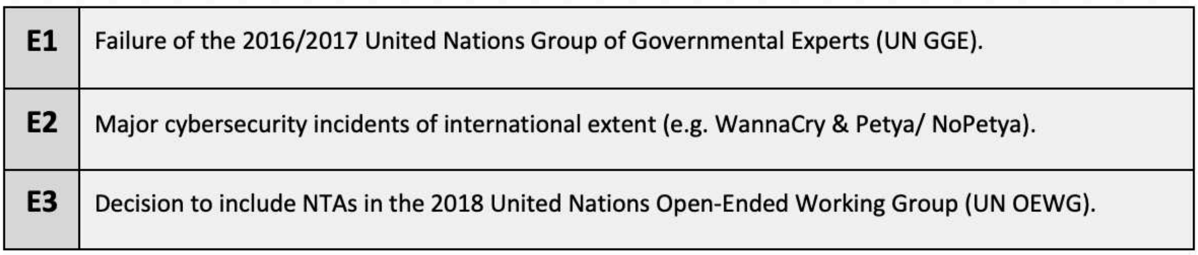
[11] The UN GGE (2019-2021) finished work in May 2021 and there are no plans for a renewal of the format so far (Geneva Internet Platform, 2021).

[12] *WannaCry* was a global ransomware attack that took place in May 2017 and hit more than 200.000 computers. It is an example of crypto-ransomware, a type of malware. Files of Microsoft Windows users were stolen by criminals. For their return, a Bitcoin ransom was demanded. The attack resulted in a tremendous financial loss (Kaspersky, 2021). *Petya* ransomware used a spreading mechanism similar to WannaCry. In 2017, Windows servers, PCs, and laptops were targeted. While Petya malware was well known before, the 2017 attack introduced a new variant: *NotPetya* (McAfee, 2021).

[13] It is interesting to note that in 2018, the Russian Federation initially proposed the creation of an Open-Ended Working Group (Delerue & Korzak, 2020).

in the causal explanation is relevant, as they significantly contributed to the rise of NTAs. The events encapsulate decisive changes in multilateral CSCB. Based on these initial results *(Phase I)*, another testing path is deduced for the following research stage *(Phase II)*.

Figure 6: Case-Specific Events



E1	Failure of the 2016/2017 United Nations Group of Governmental Experts (UN GGE).
E2	Major cybersecurity incidents of international extent (e.g. WannaCry & Petya/ NoPetya).
E3	Decision to include NTAs in the 2018 United Nations Open-Ended Working Group (UN OEWG).

The second phase involves testing another theorised cause and associated mechanism as a complementary explanatory mechanism to see whether three conjectures (**C1**, **C2**, **C3**) can sufficiently account for the most relevant causal influences on the outcome.

5.2. Causal Effects Based on Agency-Centred Historical Institutionalism

The agent-structure problem is an old controversy in International Relations theory (Wendt, 1987), as two views of preferences and institutions collide due to structural constraints (Braun, Schindler, & Wille, 2019). Neglecting agency, however, is likely to result in a struggle to explain institutional change (Emmenegger, 2021). While agency was uncommon in traditional HI, it is ubiquitous in recent scholarship (Emmenegger, 2021). Thelen describes this approach as “inject(ing) agency into institutionalist accounts in a way that rises above the particular episode in question” (2010, p. 55) while remaining in accordance with the historical institutionalist framework. DiMaggio argues that “new institutions arise when organised actors with sufficient resources […] see in them an opportunity to realise interests that they value highly” (1988, p. 14). This statement serves as the theoretical foundation for **C3**.

> *„This trend towards increased inclusion of non-state actors from the business sector and/ or civil society in global regulatory or (re-)distributive policy-making aimed at managing and solving transsovereign problems and providing global public goods can be explained by an agency-centred analysis of the interests and preferences of, and the resources available to, public and private actors.“*
>
> **Rittberger (2008, p. 20)**

The chosen approach is based on the understanding that actors remain embedded in their environment while using the room for agency to pursue their interests, which is in turn provided by existing structures. There, however, is a fundamental challenge inherent in the “paradox of plasticity” (Hall, 2016, p. 39). As soon as agency is considered, structure becomes of less causal relevance. To successfully incorporate agency in this HI approach, such agency must be contemporaneously restricted by institutions (Emmenegger, 2021). This approach is considered parallel to **C1** and **C2** and is designed to provide a sufficient explanation for the outcome by developing the idea of agency as an additional causal influence. This, again, is based on a deductive approach.

5.2.1. Conjecture 3

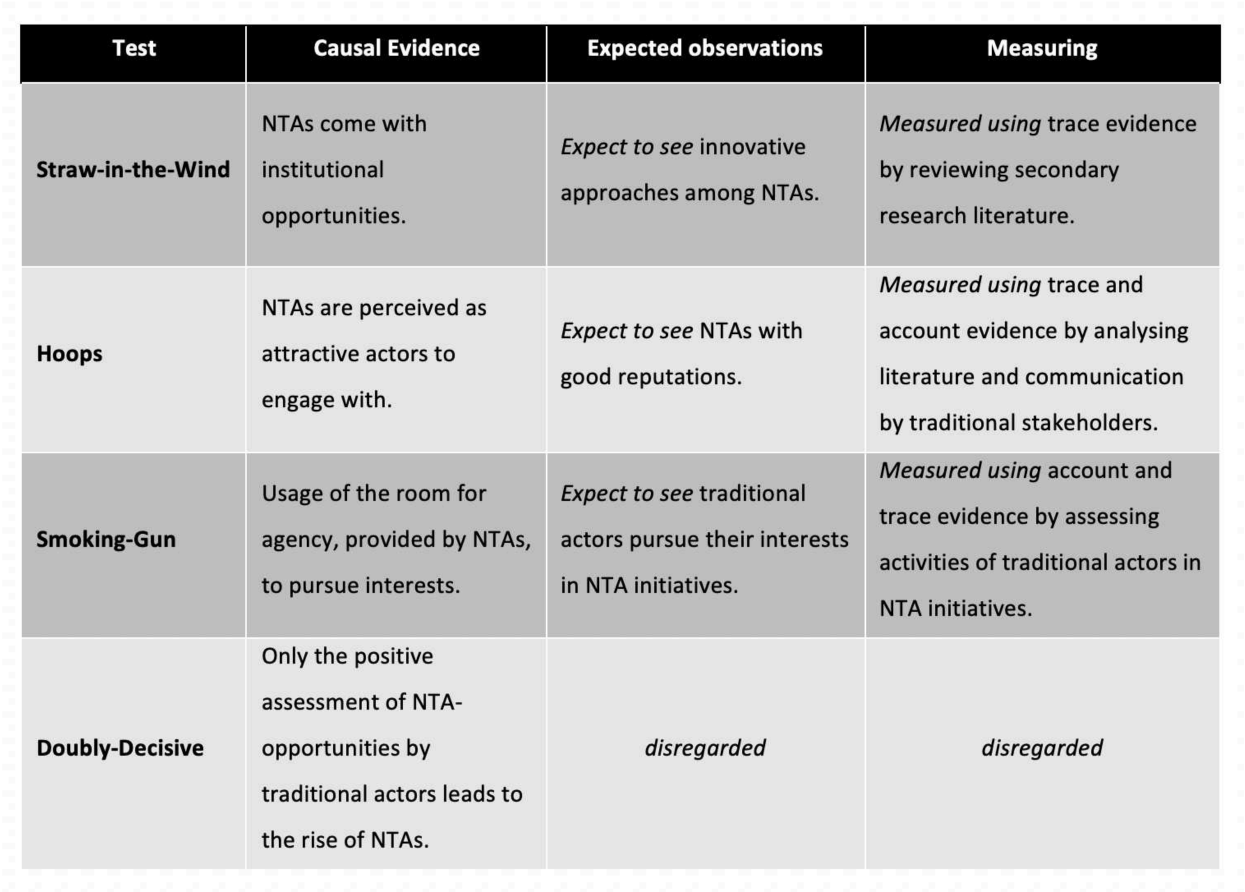
C3	**When non-traditional actors are seen as an opportunity to realise interests, *it results in the rise of non-traditional actors in multilateral Cyber Security Capacity Building.***

Unlike **C1** and **C2**, this third conjecture is derived and adapted from HI. **C3** states that when NTAs are seen as an opportunity to realise interests (IV), it results in the rise of NTAs in multilateral CSCB (DV). **C3** is based on the assumption that CSCB initiatives are – to a certain extent – designed to be consistent with the priorities of the actors behind them (Calandro & Berglund, 2019). Instead of a purely neutral endeavour, CSCB is also perceived as a “foreign policy tool used to advance […] interests (ideological, security, economic, etc.)” (Pawlak, 2016a, p. 85). Pawlak’s perspective recognises that the activities of CSCB actors are connected to agendas beyond “just” capacity-building itself. In this sense, cybersecurity governance can be promoted through CSCB, as capacity building goes in hand with a transfer of interests (Stephan, 2014; Nunnenkamp, 1995). The operationalisation of this conjecture is outlined in the following figure **(Figure 7)**.

A piece of initial **Straw-in-the-Wind Test** evidence for C3 is that NTAs come with institutional opportunities. The expected observation is the existence of innovative approaches among NTAs. Actors with different profiles have different advantages in cybersecurity governance. Traditional forums are state-centred, and participation is often limited to diplomats. Digital technologies, on the other hand, have been developed in the private sector. This dichotomy comes with consequences for traditional actors' comprehension and oversight of technologies. Coordinated action becomes even more challenging due to the allocation of competencies to separate departments or ministries (Gill, 2021).

Figure 7: Operationalisation of Conjecture 3 (C3)

C3: When non-traditional actors are seen as an opportunity to realise interests, *it results in the rise of non-traditional actors in multilateral Cyber Security Capacity Building.*



Test	Causal Evidence	Expected observations	Measuring
Straw-in-the-Wind	NTAs come with institutional opportunities.	*Expect to see* innovative approaches among NTAs.	*Measured using* trace evidence by reviewing secondary research literature.
Hoops	NTAs are perceived as attractive actors to engage with.	*Expect to see* NTAs with good reputations.	*Measured using* trace and account evidence by analysing literature and communication by traditional stakeholders.
Smoking-Gun	Usage of the room for agency, provided by NTAs, to pursue interests.	*Expect to see* traditional actors pursue their interests in NTA initiatives.	*Measured using* account and trace evidence by assessing activities of traditional actors in NTA initiatives.
Doubly-Decisive	Only the positive assessment of NTA-opportunities by traditional actors leads to the rise of NTAs.	*disregarded*	*disregarded*

Own visualisation, modified and adapted from Beach & Pedersen (2013)

Different actor profiles can be linked to specific power sources and, most importantly, actors' agencies (Calandro & Berglund, 2019). Particularly multinational companies continue to advocate for their normative ideas for CSCB (Calandro & Berglund, 2019).

> *"Rather than directly through public policy, the private sector thusly strengthens a state's ability to perform the functions of cybersecurity by setting certain technical standards while building digital infrastructures."*
>
> **Calandro & Berglund (2019, p. 5)**

While examples for such institutional opportunities of NTAs are numerous, the GFCE, the Global Commission on the Stability of Cyberspace (GCSC), and the EU CyberNet are selected as three highly relevant instances. The GFCE's core aim is to link the many separate CSCB initiatives. This comes with the opportunity to create a more resilient "global regime for strengthening cyber due diligence, defence, and resilience" (CFR, 2015). The GFCE's specific organisational structure enables this. It is designed to be an apolitical, bottom-up and unbiased forum. This, again, comes with the opportunity for traditional and non-traditional actors to exchange CSCB knowledge and share best practice projects (CFR, 2015). The GCSC comes with the opportunity "to contribute to an essential global task: supporting policy and norms coherence related to the security and stability in and of cyberspace" (GCSC, 2021). Finally, the EU CyberNet and its diverse stakeholder community allow members to "share their best practices and lessons learned in prior cyber capacity building activities or ongoing cyber actions and thereby increase the outreach to partner countries significantly" (EUCyberNet, 2021).[14] Given these examples, **C3** is initially strengthened.

Causal evidence for the **Hoops Test** is defined as the perception of NTAs as attractive actors to engage with. This is expected to be observable by looking at the reputation of NTAs. NTAs are increasingly involved in the consequences of trans-sovereign issues. Reinforced by the rising numbers, both the reputation and authority of NTAs have flourished, with traditional actors committing to NTA guidance (Abbott et al., 2016). Their relevance for international cooperation equally increases (Rittberger et al. 2008, p. 13). "At an international level, cooperation would be in the form of sharing and leveraging the results of maturity models and indices" (Hameed et al., 2018, p. 3) for the guidance of CSCB activities. Hameed et al. (2018) outline how such coordination needs ever-stronger coordination. Prominent examples for considerable and well-received NTA guided coordination are activities of the ICT4Peace Foundation, of multinational companies (e.g. Siemens, Microsoft, Deloitte), the GCSC "exceptionally important in terms of lining out and shaping the outer (non-legal) boundaries of acceptable conduct in cyberspace" (Vihul, 2013), and the GFCE (Hameed et al., 2018). Firstly, the GFCE mirrors normative principles, interests, and policy needs, making it "potentially significant" (CFR, 2015). Furthermore, the GCSC is considered as "exceptionally important in terms of lining out and shaping the outer (non-legal) boundaries of acceptable conduct in cyberspace" (Eggenschwiler, 2020). These instances show the good reputation of non-traditional actors and initiatives, which further underlines the plausibility of **C3**.

The actual usage of the room for agency provided by NTAs, by traditional actors to pursue their interests, is regarded as strong causal evidence for a **Smoking-Gun Test**. It is expected to see traditional actors pursuing their interests in NTA initiatives. According to Rittberger (2008,

[14] The *EU CyberNet stakeholder community* is part of the EU CyberNet. As a core element of the project, it strives to connect national cyber authorities, expert communities, think tanks, academic institutions, and cybersecurity organisations (EU CyberNet, 2021).

p. 20), there is an observable trend towards "institutionalised public-private cooperation within inclusive, multipartite institutions of global governance". While that general observation does not explicitly address multilateral CSCB, empirical examples show similarities. "IGO orchestration", as Abbott et al. (2016) name the process, fosters authority, legitimacy, and competitiveness of collaborating NTAs. This provides traditional actors, such as IGOs, with highly beneficial access to valuable information and additional capabilities for realising their interests (Abbott et al., 2016). The recently published UN GGE report (UNGA, 2021) addresses this room for agency for traditional actors to pursue their interests:

> *"Increased cooperation alongside more effective assistance and capacity-building in the area of ICT (Information and Communication Technology) security involving other stakeholders such as the private sector, academia, civil society and the technical community can help states apply the framework for the responsible behaviour of states in their use of ICTs. They are critical to bridging existing divides within and between states on policy, legal and technical issues relevant to ICT security."*
>
> **UNGA (2021, p. 21)**

In the new EU Cybersecurity Strategy (European Commission, 2020), the EU reiterates how it will engage with NTAs – *international partners* – to pursue their interests (Bendiek & Kettemann, 2021). This includes intensifying formats such as cyber dialogues. Their interests are explicitly stated: "strengthen(ing) the rules-based global order, promot(ing) international security and stability in cyberspace, and protect(ing) human rights and fundamental freedoms online" (European Commission, 2020, p.2). Other regional organisations, such as the AU, the OAS and the OSCE, pursue similar approaches (Hameed et al., 2018). The ITU is interested in "keeping abreast of current developments and the ever-changing requirements of the digital realm" (ITU, 2021a). This statement is directly intertwined with an emphasis on the importance of collaborating with NTAs, namely:

> *"For this reason, ITU is putting a strong emphasis on catalysing cooperation on critical issues and leveraging strategic partnerships with notable stakeholders in cybersecurity. As such, ITU facilitates beneficial synergies and maintains valuable global partnerships to enhance cybersecurity and create a safe digital environment for all."*
>
> **ITU (2021a)**

What might be the most substantial evidence for the usage of the room for agency provided by NTAs to pursue interests by traditional actors is the alignment of the GFCE with interests of the US as a cyber power (CFR, 2015). Notably, the GFCE provides essential room for agency to the US beyond mere capacity-building. The forum enables the US to "show pragmatic leadership in an area of policy need, and […] reinforces normative principles the United States has long championed" (CFR, 2015). The absence of Russia and China, as the two most important rivals of the US, in the long list of GFCE founding members further underlines this analysis (CFR, 2015). On that basis, the GFCE provides the US with the chance to move past damaged diplomatic influence and reputation as a cyber power (e.g., caused by whistle-blower Edward Snowden) (CFR, 2015).

5.2.2. Evaluation of the Combined Causal Effects

The failure of causal mechanisms based on just one theory to sufficiently explain the outcome is rather typical for research projects. For this thesis, the results of the three conjectures derived from two different theories are thus successfully used to create an eclectic process. The threefold combination provides the missing link between strictly environmental conditions and the rise of non-traditional actors in CSCB by adding the concept of (embedded) agency. Concerning the added case-specific events **(E1, E2, E3)**, it is argued that the constructed mechanism does not disregard essential aspects for the outcome (Beach & Pedersen, 2013).

It is vital to acknowledge that all assumptions remain simplifications (Lorentzen et al., 2017). While the delineated combination is designed to be case-specific, a unique outcome, and not a *case of something* (Beach & Pedersen, 2013), it can still be adapted for other cases. The theorised mechanisms **(C1, C2, C3)** are not mutually exclusive. They are pragmatically combined (Beach, 2018) to understand the causal roots of the outcome. Conclusive proof for eliminating one of them is neither sought nor provided. One of the benefits here is the familiarity with the ecosystem, resulting in the ability to include relevant case-specific events **(E1, E2, E3)** and scope conditions **(SC1, SC2, SC3)**. The analysis concludes that there are no decisive aspects of the outcome which the combined mechanism does not account for (Day & Kincaid, 1994). This is strong evidence that the complex constructed process sufficiently accounts for the rise of NTAs in multilateral CSCB. Sufficiency naturally does not claim that the combined mechanism is the only path to the outcome. It merely implies that if **C1**, **C2** and **C3** occur within the given scope conditions and in combination with the case-specific events, they are sufficient to produce it (Beach & Pedersen, 2013). George & Bennett explain that "what is left is to infer causality, which is not unsettling since many political phenomena exhibit equifinality" (2005, p.20).

6. Conclusion

Drawing on primary and secondary sources, this thesis concludes that the conceptualised process can provide a minimally sufficient explanation for the rise of NTAs in multilateral CSCB. The study's framework breaks down the process that led to the outcome in question into three scope conditions **(SC1, SC2, SC3)**, case-specific events **(E1, E2, E3)** and – most importantly – parallel conjectures **(C1, C2, C3)** which are derived from two IR theories.

The empirical analysis of the rise of NTAs in CSCB is exemplary rather than fully comprehensive. This is due to the limited scope of a bachelor thesis with a qualitative methodology. Nonetheless, it successfully provides a beneficial attempt to identify critical causal mechanisms. It can be argued that the exclusively qualitative analysis involved in the PT is indeed "a type of scientific inquiry in its own right" (Collier, 2011, p. 829). Without a doubt, further research can help refine the conjectures by a quantitative test of the proposed causal mechanisms' validity. On the theoretical side, OE helps, as Abbott et al. argue, to explain "macro-level patterns of organisational change in institutionally dynamic domains" (2016, p. 273). While Abbott et al. (2016) analysed actors in the climate ecosystem, the framework showed high transferability to the field of CSCB. Specific institutional growth dynamics and structures certainly vary. However, core concepts such as niche-finding and legitimation remain of explanatory relevance (Abbott et al., 2016).

Given that the goal of this thesis is to provide a minimally sufficient explanation, it is essential to point out that alternative theory-driven explanations might be able to account for the rise of NTAs as well. A liberal argument could be made, focusing on the role of international norms for capacity building in cyberspace. Liberal norms certainly favour human rights, international cooperation, and the rule of law (Meiser, 2018). Liberalism also provides perspectives on economic capacity building, arguing that markets arise due to human demands (Watanabe, 2020b). However: how limited is its explanatory power for the rise of NTAs? The outcome in question would be rather hard to explain from a strict realist viewpoint, as the key actors in question are non-traditional ones. In realist theory, these are not considered equally relevant.

"As more and more aspects of our lives happen online, we are becoming more vulnerable to malicious attacks. […] The frequency and scale of the attacks created a sense of urgency to improve our cybersecurity resilience."

Tasheva (2021, p. 1)

In line with these PT findings, there is undoubtedly a global need to advance non-traditional and traditional CSCB activities further. A key challenge for CSCB is bringing together heterogeneous actors with unique objectives and organisational structures by fostering a constructive relationship. This is a complex endeavour. On the one hand, it implies deciding which actors to include in specific initiatives. On the other hand, limited trust among actors is likely to result in doubts about the objectives of initiatives (Hameed et al., 2018). The underlying idea is that cybersecurity must be considered an indispensable process for and within every (non-)traditional actor. Future CSCB has to be approached inclusively and comprehensively. It is key to preserving and utilising the internet's potential as an open, global, and accessible instrument to safeguard human rights and freedom online (Geier, 2015)

> *"To this end, we need knowledge and capabilities, technical and administrative infrastructures, adequate legal frameworks, sustainable strategies and responsive policies. All of these elements must be reflected and developed in close stakeholder cooperation and consultation, and paying particular attention to local and regional contexts."*
>
> **Geier (2015, p. 16)**

This mirrors impulses for the future interconnected shape of multilateralism. The appeal? A more inclusive, "project-based multilateralism for pragmatic, problem-solving cooperation is needed" (Kortunov, 2020). "Multilateralism has to embrace the business sector, civil society and other private and public players" (Kortunov, 2020). One example is the appraisal of academic and civil society actor research for its valuable contribution of evidence-based arguments in CSCB-efforts and policy-making (Schnidrig & Aiken, 2020). The two most vital global challenges, climate change and cybersecurity need heterogenous stakeholders' flexible cooperation to achieve sustainable progress. NTAs, particularly multinational companies, are increasingly concerned about threats to their critical infrastructures due to misuse of their information or technologies (Hampson, 2017). As they continue to seek diplomatic engagement, re-evaluating forms of cooperation among traditional and non-traditional entities is essential (Eggenschwiler, 2018).

Non-traditional, multi-stakeholder partnerships should and could be established as standard practices for future multilateral arrangements (Kortunov, 2020). Pawlak (2014a) names stakeholder cooperation as one of the ten most important aspects for CSCB. It promotes good governance and leads to more inclusive outcomes with greater legitimacy. A transparent common objective is the most critical factor for successful multi-stakeholder initiatives. A better understanding of the approach NTAs pursue is crucial for their work with traditional actors. Finally, civil society organisations can best evaluate the impact of CSCB efforts (Pawlak, 2014a). Next to efficient cooperation and a common aim, one of the most important factors concerning multilateral approaches to CSCB is a (better) international coordination of activities. Efficient coordination is vital to leveraging the beneficial results of CSCB. Collett (2021) defines improved coordination as one of the four most critical issue areas for the future of CSCB. This relevance of coordination is underlined by the number of NTAs – particularly multi-stakeholders – explicitly dedicated to advancing it. The rise of NTAs has ambivalent implications. NTAs are more fragile than traditional actors, and it is critical to see their reaction to severe shocks occur in the CSCB ecosystem. They can (see **C1**) flexibly occupy niches with limited competition. However, if NTA efforts correlate with a lack of coordination, it can lead to institutional fragmentation and reduced impacts (Abbott, 2016). If NTAs continue to rise, competition will likely intensify as the amount of less dense niches decreases. This may result in new NTA strategies, such as occupying entire issue areas. Looking back at established NTAs, prominently the GFCE, this can already – somewhat – be observed today. The critical question of legitimacy regarding the growing influence of NTAs in international politics cannot be disregarded either (Philipps & Braun, 2020).

On the contrary, NTAs reinforce traditional public governance with new but complementary mechanisms and standards (Abbott et al., 2016). The rise of NTAs provides a "wealth of natural experiments" (Abbott et al., 2016, p. 272) that traditional actors can learn from. Non-traditional formats enable new opportunities for different types of NTAs to participate in multilateral governance. With the right preconditions, such forms of cooperation can be a genuinely beneficial development for the existing multilateral order (Philipps & Braun, 2020). This comes with implications for non-traditional and traditional actors alike. Specific implications for Germany's role in CSCB are addressed in detail (see **Annexe 4**). Public-private synergies rely on the consistency of NTAs with underlying norms. It is essential that NTAs are not established as rivals to existing traditional actors. Instead, they should be designed to elevate their effectiveness (Abbott et al., 2016). Most importantly, NTAs "can act when divergent interests block intergovernmental agreement" (Abbott et al., 2016, p. 272). This becomes highly relevant in the face of cyber threats and aggressions between traditional global powers such as the US, Russia, and China.

Further (comparative) research could explore the explanatory power of OE theory in other relevant issue areas. Elevated by the COVID-19 pandemic, this most prominently is global public health. A quick view on the differences and similarities of Abbott et al.'s work on climate governance compared to the field of CSCB already allows first insights to this regard (2016). An in-depth examination of the underlying causes for identified differences is equally intriguing. One approach might be asking whether the more explicit security character of CSCB restrains NTAs due to security being at the very heart of (traditional) state competency.

> *"The question of regular multi-stakeholder participation promises to become a pressing issue for states. Institutionalised multi-stakeholder participation in the international cybersecurity debate might be a genie that will be hard to put back into the bottle."*
>
> **Delerue & Korzak (2020)**

This thesis shows that, even though international CSCB is a young field, it has a sufficient track record to identify and analyse relevant trends. There is still comparatively little literature on such dynamics, as experts and practitioners often lack the time for thorough reflection. The potential to provide actors across the CSCB ecosystem with new insights makes this thesis a valuable contribution to the state of research. In sum, the field of CSCB is still new and constantly emerging. The future will show how the role of NTAs will develop in this policy field. Engagement across (non-)traditional actors and perspectives, as part of a more efficient international coordination and public-private cooperation, can lead to more sustainable, impactful and intelligent CSCB. An embrace of this approach is set to significantly impact future CSCB initiatives and policies (Schnidrig & Aiken, 2020).

OE, complemented by an agency-centred HI perspective on micro-foundations, finally proves to constitute a valuable theoretical framework for analysing organisational design and behaviour. What theories will be sufficient for explaining future CSCB dynamics may change. But as of the current state of CSCB, it is coined by the rise of NTAs. This is the institutional outcome of a dynamic process, shaped by the flexibility of NTAs to choose favourable niches, the beneficial interaction of NTAs with traditional actors, and finally, the perception of NTAs as an opportunity to realise interests by traditional actors.

References

Abbott, K. W. (2012). The Transnational Regime Complex for Climate Change. *Government and Policy 30*(4), 571-590.

Abbott, K. W., Green, J. F., & Keohane, R. O. (2016). *Organizational Ecology and Institutional Change in Global Governance*. New York, USA: Cambridge University Press.

Allison, G. T. (1971). *Essence of Decision. Explaining the Cuban Missile Crisis*. Boston: Little, Brown and Company.

APC (2019). *APC statement at the Intersessional Meeting of the Open-ended Working Group on ICTs: Engaging all stakeholders to enhance capacity-building efforts*. Retrieved from https://www.apc.org/en/node/35932 (11 December 2021).

ASPI (2015). *Cyber Maturity in the Asia-Pacific Region 2015*. Canberra, AUS: ASPI. Retrieved from https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2015 (11 December 2021).

Austin, G. (2018). *Cybersecurity in China: The Next Wave*. Cham, CH: Springer.

Beach, D. (2018). Process Tracing Methods. In C. Wagemann, A. Goerres, & M. Siewert (Eds.), *Handbuch Methoden der Politikwissenschaft* (pp. 1-21). Wiesbaden: Springer Fachmedien Wiesbaden.

Beach, D., & Pedersen, R. (2012). Case selection strategies in Process-tracing research and the Implications of Taking the Study of Causal Mechanisms Seriously. *SSRN Electronic Journal*. Retrieved from https://dpsa.dk/papers/Case%20selection%20in%20PT%20-%20Beach%20and%20Pedersen%20-%202nd%20draft%281%29%281%29.pdf (19 December 2021).

Beach, D., & Pedersen, R. (2013). *Process-Tracing Methods: Foundations and Guidelines*. Ann Arbor, MI: University of Michigan Press.

Bei, K. (2020). Coordinating a Global Network for Cyber Capacity Building. *Global Cyber Expertise Magazine, 69* (8), 58-61. Retrieved from https://thegfce.org/wp-content/uploads/2020/12/Global-Cyber-Expertise-Magazine-Issue-8.pdf (17 December 2021).

Bendiek, A., & Kettemann, M. C. (2021). Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy. *SWP Comment, 16*. Retrieved from https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf (14 December 2021).

Bennett, A., & Checkel, J. T. (2014). *Process Tracing: From Metaphor to Analytic Tool*. Cambridge, UK: Cambridge University Press.

Braun, B., Schindler, S., & Wille, T. (2019). Rethinking agency in International Relations: performativity, performances and actor-networks. *Journal of International Relations and Development, 22*(4), 787-807.

Broeders, D. (2017). Aligning the international protecction of „the public core of the internet" with state sovereignty and national security. *Journal of Cyber Policy, 2*(4), 1-11. Retrieved from https://www.researchgate.net/publication/321237654_Aligning_the_international_protection_of_%27the_public_core_of_the_internet%27_with_state_sovereignty_and_national_security (14 December 2021).

Bulkeley, H. et al. (2012). Governing Climate Change Transnationally: Assessing the Evidence from a Database of Sixty Initiatives. *Government and Policy 30*(4), 591-612.

Bull, B., Bøås, M., & McNeill, D. (2004). Private Sector Influence in the Multilateral System: A Changing Structure of World Governance? *Global Governance, 10(*4), 481-498. Retrieved from http://www.jstor.org/stable/27800543 (17 December 2021).

Calandro, E., & Berglund, N. (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case. 2019 *GIGANet Conference Paper*. Retrieved from https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf (11 December 2021).

Calderaro, A., & Craig, A. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly 41,* 917 - 938.

CFR (2015). *The Global Forum on Cyber Expertise: Its Policy, Normative, and Political Importance*. Retrieved from https://www.cfr.org/blog/global-forum-cyber-expertise-its-policy-normative-and-political-importance (11 December 2021).

Checkel, J. T. (2005). International Institutions and Socialization in Europe: Introduction and Framework. *International Organization, 59*(4), 801-826. Retrieved from http://www.jstor.org/stable/3877829 (14 December 2021).

Clark, D., Berson, T. & Lin, H. (2014). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, DC: National Academic Press.

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy,* 1-20. Retrieved from https://www.tandfonline.com/doi/epub/10.1080/23738871.2021.1948582?needAccess=true (19 December 2021).

Collett, R., & Barmpaliou, N. (2021). *International Cyber Capacity Building: Global Trends and Scenarios*. Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf (19 December 2021).

Collier, D. (2011). Understanding Process Tracing. *PS: Political Science and Politics, 44*(4), 823-830.

Connolly, P. M. (2007). *Deeper Capacity Building for Greater Impact*. Retrieved from https://capacitycanada.ca/wp-content/uploads/2014/09/Deeper-Capacity-Building-for-Greater-Impact.pdf (17 December 2021).

Creese, S. et al. (2021). The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions. *Personal and Ubiquitous Computing, 25*, 941-955.

Crespo, L., Wanner, B., & Ghernaouti, S. (2018). *Cybersecurity Capacity Building: A Swiss Approach*. Wiesbaden, DE: Springer VS.

CRI (2021). *About CRI: The Cyber Risk Institute*. Retrieved from https://cyberriskinstitute.org/about/ (17 December 2021).

Cybil Portal (2021a). *Actor: International Telecommunication Union (ITU)*. Retrieved from https://cybilportal.org/actors/international-telecommunication-union-itu/ (19 December 2021).

Cybil Portal (2021b). *Actors. Profiles of governments, companies, organisations and other actors involved in international cyber capacity building*. Retrieved from https://cybilportal.org/actors/ (14 December 2021).

Delerue, F., & Korzak, E. (2020). *From Multilateral to Multistakeholder? New Developments in UN Processes on Cybersecurity. Digital and Cyberspace Policy Program*. Retrieved from https://www.cfr.org/blog/multilateral-multistakeholder-new-developments-un-processes-cybersecurity (14 December 2021).

DiMaggio, P. (1988). Interest and agency in institutional theory. In L. Zucker (Ed.), *Institutional patterns and organizations: Culture and environment* (pp. 3-21). Massachusetts: Ballinger Publishing.

DiMaggio, P., Powell, W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48*, 147–160. Retrieved from https://link.springer.com/content/pdf/10.1007%2F978-3-658-08184-3_17.pdf (11 December 2021).

Drezner, D. W. (2010). Afterword. Is historical institutionalism bunk? *Review of International Political Economy, 17*(4), 791-804. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/09692291003723656 (11 December 2021).

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*, 32-35.

Dutton, W.H. (2015). Multistakeholder Internet Governance? *Quello Center Working Paper, 2615596*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615596 (19 December 2021).

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy, 9* (2019), 280-306. Retrieved from https://www.researchgate.net/publication/338803905_Cybersecurity_Capacity_Does_It_Matter (19 December 2021).

Eggenschwiler, J. (2018). A Typology of Cybersecurity Governance Models. *St Antony's International Review, 13*(2), 64-78. Retrieved from https://www.jstor.org/stable/26501049 (17 December 2021).

Eggenschwiler, J. (2019). International Cybersecurity Norm Development: The Roles of States Post-2017. *Research In Focus, EU Cyber Direct*. Retrieved from https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/Ec69VU7n/jacqueline-eggenschwiler-international-norm-development-roles-of-state-april-2019-eucyberdirect.pdf (17 December 2021).

Eggenschwiler, J. (2020). Expert commissions and norms of responsible behaviour in cyberspace: a review of the activities of the GCSC. *Digital Policy, Regulation and Governance, 22*(2), 93-107.

Elling, B. (2008). *Rationality and the Environment. Decision-making in Environmental Politics and Assessment*. London, UK/ Sterling, VA: Routledge.

Emmenegger, P. (2021). Agency in historical institutionalism: Coalitional work in the creation, maintenance, and change of institutions. *Theory and Society, 50*(4), 607-626.

ENISA (2021). *European Union Agency for Cybersecurity (ENISA) Mandate and Regulatory Framework*. Retrieved from https://www.enisa.europa.eu/about-enisa/regulatory-framework (19 December 2021).

EPRS (2020). *Non-exhaustive mapping of cyber stakeholders.* EP Think Tank: European Parliamentary Research Service (EPRS). Retrieved from https://epthinktank.eu/2020/05/29/understanding-the-eus-approach-to-cyber-diplomacy-and-cyber-defence/non-exhaustive-mapping-of-cyber-stakeholders/ (14 December 2021).

EU CyberNet (2021). *Stakeholder Community. We bring together the stakeholders of EU's cybersecurity*. Retrieved from https://www.eucybernet.eu/stakeholder-community/ (14 December 2021).

European Commission (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164 (11 December 2021).

Farrell, H., & Newman, A. L. (2014). *Domestic Institutions beyond the Nation-State: Charting the New Interdependence Approach*. Cambridge, UK: Cambridge University Press.

Federal Ministry of the Interior (2021). Cybersecurity Strategy for Germany. Retrieved from https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1 (17 December 2021).

Finnemore, M. (1996). *Norms, culture, and world politics: insights from sociology's institutionalism*. New York, USA: Cambridge University Press.

Fioretos, O. (2011). *Historical Institutionalism in International Relations*. New York, NY: Cambridge University Press.

FIRST (2021). *About FIRST*. Retrieved from https://www.first.org/about/ (17 December 2021).

Ganghof, S. (2016). Forschungsdesign in der Politikwissenschaft - Kausale Perspektiven versus kontrastive Theorietests. *Austrian Journal of Political Science, 45*, 1-12.

GCSC (2021). *The Commission*. Retrieved from https://cyberstability.org/about/ (19 December 2021).

GCSCC (2021a). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Retrieved from https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf (14 December 2021).

GCSCC (2021b). *Cybil: The Cyber Capacity Knowledge Portal*. Retrieved from https://gcscc.ox.ac.uk/cybil-knowledge-portal (14 December 2021).

Geier, K. (2015). *How Effective are International Approaches for Global Cyber Security?* Retrieved from https://vdw-ev.de/wp-content/uploads/2015/11/Geier-K.-International-Approaches-for-Global-Cyber-Security.-CyberwarCyberpeace-24.10.2015.pdf (17 December 2021).

Geneva Internet Platform (2021). UN GGE and OEWG. *digwatch*. Retrieved from https://dig.watch/processes/un-gge/ (19 December 2021).

GFCE (2018). *Cyber Security Initiative in OAS member states*. Retrieved from https://thegfce.org/initiatives/cyber-security-initiative-in-oas-member-states/ (19 December 2021).

Gill, A. S. (2021). The changing role of multilateral forums in regulating armed conflict in the digital age. *IRRC, 913*. Retrieved from https://international-review.icrc.org/articles/changing-role-multilateral-forums-regulating-armed-conflict-digital-age-913 (19 December 2021).

Global Cyber Alliance (2021). *Capacity & Resilience*. Retrieved from https://www.globalcyberalliance.org/capacity-resilience/ (17 December 2021).

GPD (2020). *Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers*. Retrieved from https://www.gp-digital.org/wp-content/uploads/2020/08/NCSS-guidance-doc_gpd.pdf (19 December 2021).

Hall, P. A. (2016). Politics as a Process Structured in Space and Time. In O., Fioretos, J., Lynch & A., Steinhouse (Eds.). *The Oxford Handbook of Historical Institutionalism* (pp. 31-50). New York, NY: Oxford University Press.

Hameed, F., Agrafiotis, I., Weisser, C., Goldsmith, M., & Creese, S. (2018). Analysing trends and success factors of international cybersecurity capacity-building initiatives. *SECURWARE 2018: The Twelfth International Conference on Emerging Security Information, Systems and Technologies*. Retrieved from https://ora.ox.ac.uk/objects/uuid:50e9c5aa-4f3d-40f0-a0a0-ff538b735291 (19 December 2021).

Hampson, H. Getting beyond Norms: New Approaches to International Cyber Security Challenges. Centre for International Governance Innovation. Retrieved from https://lib.ugent.be/en/catalog/ebk01:3810000000348542 (19 December 2021).

Hannan, M. T. (2005). Ecologies of Organizations: Diversity and Identity. *Journal of Economic Perspectives, 19(*1), 51-70. Retrieved from https://www.aeaweb.org/articles?id=10.1257/0895330053147985 (14 December 2021).

Hannan, M. T., & Freeman, J. (1984). *Structural Inertia and Organizational Change*. Albany, NY: American Sociological Association.

Hannan, M. T., & Freeman, J. (1977). *The Population Ecology of Organizations*. Chicago, IL: University of Chicago Press.

Hathaway, M. (2013). *Cyber Readiness Index 1.0*. Cambridge, MA: Belfer Center for Science and International Affairs.

Hathaway, M. (2015). *Cyber Readiness Index 2.0. A Plan for Cyber Readiness: A Baseline and an Index*. Washington, DC: Potomac Institute for Policy Studies.

Heeks, R. (2014). New Priorities for ICT4D: Policy, Practice and WSIS in a Post-2015 World. *Development Informatics Working Paper Series, 59*(2014). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3438431 (11 December 2021).

Hewlett Foundation (2021). *Cyber*. Retrieved from https://hewlett.org/strategy/cyber/ (11 December 2021).

Hohmann, M., Pirang, A., & Benner, T. (2017). *Advancing Cybersecurity Capacity Building. Implementing a Principle-Based Approach*. Retrieved from https://www.gppi.net/media/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf (19 December 2021).

Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society, 33*(2), 224–242.

Hui, P., Bruce, J., Fink, G., Gregory, M., Best, D., McGrath, L. (2010). Towards Efficient Collaboration in Cyber Security. *Conference on Collaborative Technologies and Systems (CTS)*. Retrieved from https://www.researchgate.net/publication/224143314_Towards_efficient_collaboration_in_cyber_security (17 December 2021).

Humphreys, M., & Jacobs, A. M. (2015). Mixing Methods: A Bayesian Approach. *American Political Science Review, 109*(4), 653-673.

ITU (2021a). *Global Partnership*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-partnership.aspx (17 December 2021).

ITU (2021b). *ITU-D Capacity Development: Develop skills and knowledge to become a competent digital citizen*. Retrieved from https://www.itu.int/itu-d/sites/capacity-development/ (19 December 2021).

ITU (2021c). *ITU-D Cybersecurity: Facilitating a trusted cyberspace for all*. Retrieved from https://www.itu.int/itu-d/sites/cybersecurity/ (19 December 2021).

Kaspersky (2021). What is WannaCry ransomware? Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (14 December 2021).

Keohane, R. O. (2017). *Observations on the Promise and Pitfalls of Historical Institutionalism in International Relations*. Oxford, UK: Oxford University Press.

Klimburg, A., & Zylberberg, H. (2015). Cyber Security Capacity Building: Developing Access. *NUPI Report, 6*(2015). Retrieved from https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf (14 December 2021).

Kortunov, A. (2020). *Multilateralism Needs Reinventing, Not Resurrecting*. Retrieved from https://peacelab.blog/2020/12/multilateralism-needs-reinventing-not-resurrecting (14 December 2021).

Kulesza, J., & Eggenschwiler, J. (2020). Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace. In D., Broeders & B., van den Berg (Ed.). *Governing Cyberspace. Behavior, Power, and Diplomacy* (pp. 245-262). London: Rowman & Littlefield.

Lango, H.-I. (2016). Cyber Security Capacity Building: Security and Freedom. *NUPI Report, 1*(2016). Retrieved from https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2381169/NUPI_Report_1_16_Hans_Inge%2bLango.pdf?sequence=3&isAllowed=y (11 December 2021).

Let'sTalkCyber (2021). *Let's Talk Cyber*. Retrieved from https://letstalkcyber.org (11 December 2021).

Lété, B. (2021). *Implementing the EU Cybersecurity Strategy. Recommendations From The European Cyber Agora*. Retrieved from https://www.gmfus.org/sites/default/files/2021-10/Cyber-Agora-20page-web-02.pdf (17 December 2021).

Lorentzen, P. et al. (2017). Qualitative investigation of theoretical models: the value of process tracing. *Journal of Theoretical Politics 29*(3), 467-491.

Mahoney, J. (2012). The Logic of Process Tracing Tests in the Social Sciences. *SAGE journals, 41*(4), 570-597. Retrieved from https://journals.sagepub.com/doi/10.1177/0049124112437709 (17 December 2021).

Malcolm, J. (2017). *EFF at Cyberspace Events in Delhi: Protecting the Public Core of the Internet*. Retrieved from https://www.eff.org/de/deeplinks/2017/11/eff-cyberspace-events-delhi-protecting-public-core-internet (13 December 2021).

Maurer, T., & Nelson, A. (2020). International Strategy to Better Protect the Financial System Against Cyber Threats. *Carnegie Endowment for International Peace*. Retrieved from https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf (16 December 2021).

McAfee (2021). *What Is Petya and NotPetya Ransomware?* Retrieved from https://www.mcafee.com/enterprise/de-de/security-awareness/ransomware/petya.html (19 December 2021).

Meiser, J. W. (2018). Introducing Liberalism in International Relations Theory. Retrieved from https://www.e-ir.info/2018/02/18/introducing-liberalism-in-international-relations-theory/ (17 December 2021).

Microsoft (2021). *Microsoft Security*. Retrieved from https://www.microsoft.com/en-us/security/business/government (18 December 2021).

Müller, B., & Kremer, J.-F. (2013). *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin/ Heidelberg, DE: Springer.

Nasiritousi, N., Hjerpe, M., & Linnér, B.-O. (2016). The roles of non-state actors in climate change governance: understanding agency through governance profiles. *International Environmental Agreements: Politics, Law and Economics, 16*(1), 109-126. Retrieved from https://link.springer.com/article/10.1007/s10784-014-9243-8 (18 December 2021).

Nikolova, I. (2017). Best Practice for Cybersecurity Capacity Building in Bulgaria’s Public Sector. *Information & Security: An International Journal 38* (2017), 79-92. Retrieved from https://isij.eu/article/best-practice-cybersecurity-capacity-building-bulgarias-public-sector (18 December 2021).

Nunnenkamp, P. (1995). What donors mean by good governance. *IDS Bulletin, 29*(9), 1527-1552.

OECD (2015). Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document. Retrieved from https://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm (15 December 2021).

Orban, A., & Trampusch, C. (2019). Fallstudien und Methoden. In H., Obinger, M. Schmidt (Eds.). *Handbuch Sozialpolitik* (pp. 361-381). Wiesbaden: Springer VS.

Pawlak, P. (2014a). Cyber Capacity Building in Ten Points. *European Union Institute for Security Studies Conference on Cyber Capacity Building Paris 2014*. Retrieved from https://www.combattingcybercrime.org/files/virtual-library/capacity-building/cyber-capacity-building-in-ten-points.pdf (20 December 2021).

Pawlak, P. (2014b). Riding the digital wave. The impact of cyber capacity building on human development. *ISSUE, 21*. Retrieved from https://www.files.ethz.ch/isn/186860/Report_21_Cyber.pdf (12 December 2021).

Pawlak, P. (2016a). Capacity Building in Cyberspace as an Instrument of Foreign Policy. *Global Policy 7(*1), 83-92.

Pawlak, P. (2016b). Confidence-Building Measures in Cyberspace: Current Debates and Trends. In A.-M., Osula, H. Rõigas (Eds.). *International Cyber Norms: Legal, Policy & Industry Perspectives* (pp. 129-153). Retrieved from https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch7.pdf (18 December 2021).

Pawlak, P., & Barmpaliou, P.-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy, 2* (1), 123-144. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1294610 (10 December 2021).

Pawlak, P., & Missiroli, A. (2019). Introduction: Trends, Patterns and Challenges for International Cooperation in Cyberspace. *European Foreign Affairs Review, 24*(2), 125-133. Retrieved from https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/24.2/EERR2019008 (10 December 2021).

Philipps, L., & Braun, D. (2020). The Future of Multilateralism. *KAS International Reports.* Retrieved from https://www.kas.de/documents/259121/10240919/The+Future+of+Multilateralism.pdf/6ad20720-e21f-7986-b784-ec6729adc53f?version=1.0&t=1601545054776 (18 December 2021).

Pijnenburg Muller, L. (2015). Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities. *NUPI Report, 3*(2015). Retrieved from https://cybilportal.org/wp-content/uploads/2020/06/NUPIReport03-15-Muller.pdf (15 December 2021).

Radunović, V., & Rüfenacht, D. (2016). *Cybersecurity Competence Building Trends*. Retrieved from https://issuu.com/diplo/docs/cybersecurity_full_report (19 December 2021).

Reitinger, P. (2011). *Enabling Distributed Security in Cyberspace. Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Retrieved from https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf (14 December 2021).

Ricks, J. I., & Liu, A. H. (2018). Process-Tracing Research Designs: A Practical Guide. *PS: Political Science & Politics, 51*(4), 842-846.

Risse, T. (2012). Governance Configurations in Areas of Limited Statehood. *SFB-Governance Working Paper Series, 32*. Retrieved from https://www.sfb-governance.de/en/publikationen/sfb-700-working_papers/wp32/SFB-Governance-Working-Paper-32.pdf (14 December 2021).

Rittberger, V. (2008). Global Governance: From ‚Exclusive' Multilateralism to Inclusive Multipartite Institutions. *Tübinger Arbeitspapiere zur Internationalen Politik und Friedensforschung, 52*. Tübingen. Retrieved from https://d-nb.info/1167408160/34 (18 December 2021).

Rohlfing, I. (2014). Comparative Hypothesis Testing via Process Tracing. *Sociological Methods & Research, 43*, 606-642.

Rozentāle, L. (2021). Launching the European Cyber Agora. *EU Policy Blog*. Retrieved from https://blogs.microsoft.com/eupolicy/2021/03/25/launching-the-european-cyber-agora/ (17 December 2021).

Rüland, J. (2018). "Principled Multilateralism" versus "Diminished Multilateralism:" Some General Reflections. In C., Echle, P., Rueppel, M., Sarmah & Y. L., Hwee. *Multilateralism in a Changing World Order* (pp. 1-12). Singapore: Konrad-Adenauer-Stiftung.

Ruhl, C., Hollis, D., Hoffman, W., Maurer, T. (2020). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Carnegie Endowment for International Peace & Perry World House Working Paper. Retrieved from https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf (18 December 2021).

Rupp, C., & Herpig, S. (2021). *Germany's Cybersecurity Architecture*. Retrieved from https://www.stiftung-nv.de/sites/default/files/7thed_cybersecurityarchitecture.pdf (11 December 2021).

Schia, N. (2016). „Teach a person how to surf": Cyber security as development assistance. *NUPI Report, 4*(2016). Retrieved from https://www.files.ethz.ch/isn/196649/NUPI_Report_4_16_Nagelhus_Schia.pdf (13 December 2021).

Schimmelfennig, F. (2001). The Community Trap: Liberal Norms, Rhetorical Action, and the Eastern Enlargement of the European Union. *International Organization, 55*(1), 47-80.

Schnidrig, D., & Aiken, K. (2020). Stakeholder Engagement in Cyber Capacity Building - Lessons Learned After 5 Years of GFCE. *Global Cyber Expertise Magazine, 57(*7). Retrieved from https://thegfce.org/wp-content/uploads/2020/04/Global-Cyber-Expertise-Magazine_edition7_April2020.pdf (14 December 2021).

School, O. M. (2021). *The Global Cyber Security Capacity Centre*. Retrieved from https://www.oxfordmartin.ox.ac.uk/cyber-security/ (16 December 2021).

Schroeder, H., & Lovell, H. (2012). The role of non-nation-state actors and side events in the international climate negotiations. *Climate Policy 12*, 23-37.

Seyle, C., Weiss, T. G., & Coolidge, K. (2013). *The Rise of Non-State Actors in Global Governance: Opportunities and Limitations*. Retrieved from https://oneearthfuture.org/research-analysis/rise-non-state-actors-global-governance-opportunities-and-limitations (18 December 2021).

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

SPD, Greens, & FDP (2021). *Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit*. Retrieved from https://www.tagesspiegel.de/downloads/27829944/1/koalitionsvertrag-ampel-2021-2025.pdf (19 December 2021).

Stadnik, I. (2018). *WS 9: Non-state actors in Europe and beyond: The true shapers of cybersecurity norms?!* EuroDIG European Dialogue on Internet Governance 2018. Retrieved from https://comment.eurodig.org/eurodig-2018-messages/ws-9-non-state-actors-in-europe-and-beyond-the-true-shapers-of-cybersecurity-norms/ (18 November 2021).

Stephan, S. et al. (2014). School Mental Health: The Impact of State and Local Capacity-Building Training. *International Journal of Education Policy & Leadership, 9*(7).

Tasheva, I. (2021). Cybersecurity post-COVID-19: Lessons learned and policy recommendations. European View. Retrieved from https://journals.sagepub.com/doi/full/10.1177/17816858211059250 (21 December 2021).

Thelen, K. (2010). Beyond comparative statics: Historical institutional approaches to stability and change in the political economy of labor. In G., Morgan et al. (Eds.). The Oxford handbook of comparative institutional analysis (pp. 41-61). Oxford, UK: Oxford University Press.

Tiirmaa-Klaar, H. (2016). Building National Cyber Resilience and Protecting Critical Information Infrastructure. *Journal of Cyber Policy 1*(1), 94-106.

UNGA (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. Retrieved from https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf (12 November 2021).

UN OEWG (2021). Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (19 December 2021).

Valeriano, B., & Maness, R. (2018). International relations theory and cyber security: Threats, conflicts, and ethics in an emergent domain. In C., Brown & R., Eckersley. The Oxford Handbook of International Political Theory (pp. 259-272). Oxford, UK: Oxford University Press.

Vihul, L. (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare. *Blog of the European Journal of International Law (EIJL: Talk!)*. Retrieved from https://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/ (13 December 2021).

Voeten, E. (2019). Making Sense of the Design of International Institutions. *Annual Review of Political Science 22*(1), 147-163. Retrieved from https://www.annualreviews.org/doi/abs/10.1146/annurev-polisci-041916-021108 (18 December 2021).

von Bernstorff, J. (2007). Non-State Actors in law-making and in the shaping of policy. On the legality and legitimacy of NGO participation in international law. *Study for the preparation of the Konrad-Adenauer-Foundation's Conference on International Law 2007*. Retrieved from https://www.kas.de/c/document_library/get_file?uuid=4e2e1560-2408-8bfd-9f85-5dea3e38c200&groupId=252038 (14 December 2021).

Watanabe, S. (2020a). States' Capacity Building for Cybersecurity: An IR Approach. Cham, CH: Springer.

Watanabe, S. (2020b). Strategic Analysis of Capacity Building fort the Cyber Security of the United States in Asia. *Jurnal Asia Pacific Studies, 4*(2), 100-111.

Waz, J., & Weiser, P. (2012). Internet Governance: The Role of Multistakeholder Organizations. *Journal on Telecommunications & High Technology Law, 10*. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/jtelhtel10&div=25&id=&page= (16 December 2021).

Wendt, A. E. (1987). The Agent-Structure Problem in International Relations Theory. *International Organization, 41*(3), 335-370. Retrieved from http://www.jstor.org/stable/2706749 (12 December 2021).

Wight, C. (2004). Theorizing the Mechanisms of Conceptual and Semiotic Space. *Philosophy of the Social Sciences, 34*(2), 283-299.

Wilén, N. (2009). Capacity-Building or Capacity-Taking? Legitimizing Concepts in Peace and Development Operations. *International Peacekeeping 16*(3), 337-351.

Wood, E. J. (2003). *Insurgent Collective Action and Civil War in El Salvador*. Cambridge, UK: Cambridge University Press.

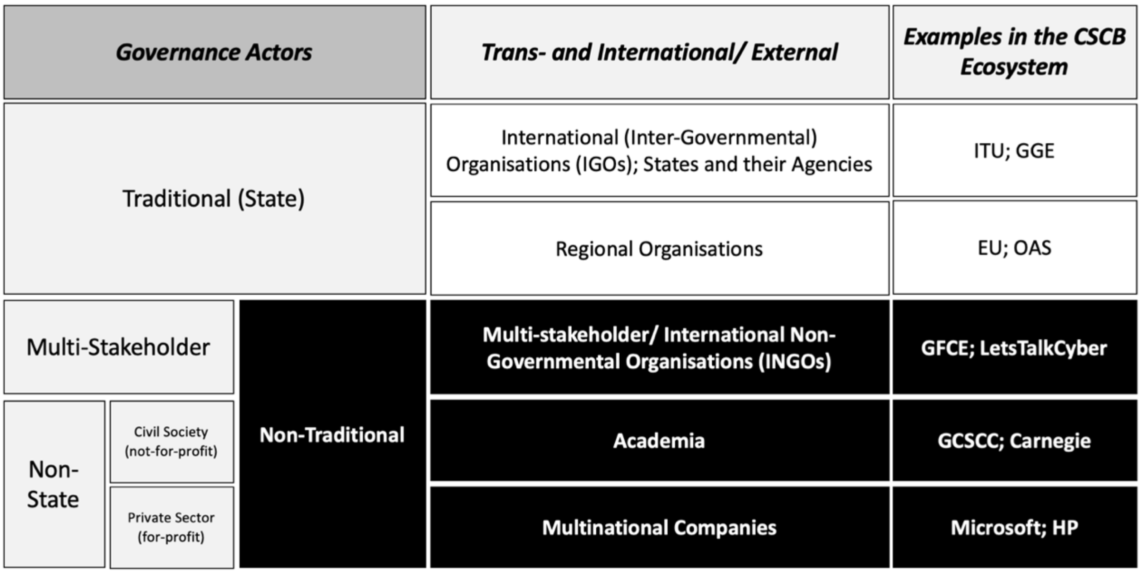
World Bank Group (2016). World Development Report 2016: Digital Dividends. Retrieved from https://www.worldbank.org/en/publication/wdr2016 (17 December 2021).

World Economic Forum (2012). Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. Retrieved from https://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf (19 December 2021).

World Economic Forum (2020). The Global Risks Report 2020, 15. Retrieved from https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (17 December 2021).

Annexe

Annexe 1: Non-Traditional Actors (NTAs)

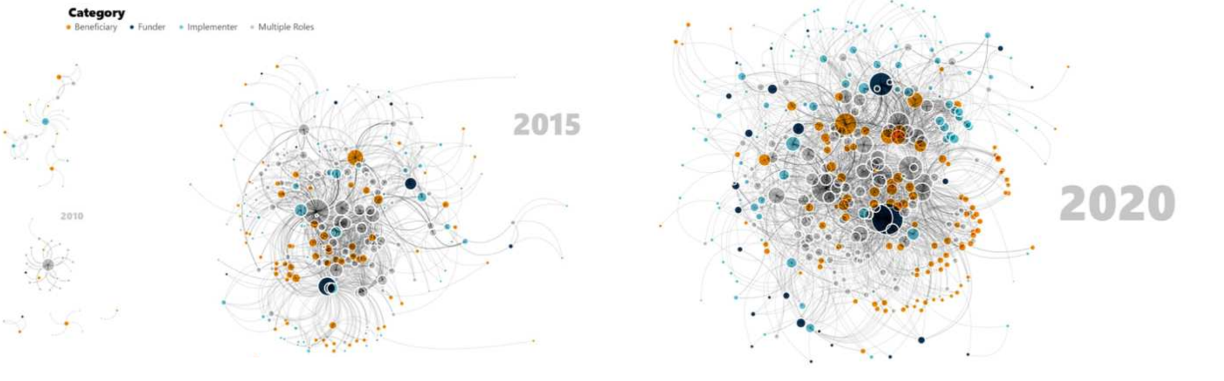


Governance Actors			*Trans- and International/ External*	*Examples in the CSCB Ecosystem*
Traditional (State)			International (Inter-Governmental) Organisations (IGOs); States and their Agencies	ITU; GGE
			Regional Organisations	EU; OAS
Multi-Stakeholder		Non-Traditional	**Multi-stakeholder/ International Non-Governmental Organisations (INGOs)**	**GFCE; LetsTalkCyber**
Non-State	Civil Society (not-for-profit)		**Academia**	**GCSCC; Carnegie**
	Private Sector (for-profit)		**Multinational Companies**	**Microsoft; HP**

Own visualisation adapted according to Risse (2012, p.9)

Annexe 2: The Growing CSCB Actor Network

FIGURE 5. **CCB ACTORS NETWORK**
2010, 2015, and 2020



Data: Cybil Portal, 2021

Retrieved from Collett & Barmpaliou (2021, p.21)

Annexe 3: Selection of Empirical Examples

Conjecture	Empirical Examples
C1	*e.g., Cybil Portal, UN OEWG, GPD, Global Cyber Alliance, CRI, Hewlett Foundation, ENISA, ITU, GFCE, ICT4Peace*
C2	*e.g., Commonwealth Cyber Declaration Programme, Let'sTalkCyber, DDP, Microsoft, Cyber Agora, GFCE, Huawei, Siemens, Hewlett Foundation*
C3	*e.g., GFCE, GCSC, EU CyberNet, ICT4Peace, Siemens, Microsoft, Deloitte, AU, OAS, OSCE, ITU, US, Russia, China*

Own visualisation (see Selection of Empirical Data & Empirical Analysis)

Annexe 4: Implications for Germany's Role in CSCB

> *"Building confidence and creating stability in the use of ICTs requires public actors to live up to their traditional roles as standard-setters and enforcers of norms and take on additional roles, e.g. as sparring partners of non-state initiatives or meta-level orchestrators of normative responsibilities."*
>
> **Eggenschwiler (2019, p.1)**

What role for traditional (state) actors in CSCB? As apparent with this study *(Multilateral Approaches to Cyber Security Capacity Building: The Rise of Non-Traditional Actors)*, an increasing share of CSCB activity stems from NTAs, rather than from traditional, sovereign entities such as IGOs and states. A trend that is likely to intensify in the future. "The current lack of global technology governance and the presence of cybersecurity blind spots" (World Economic Forum, 2020, p. 61) simultaneously increase the risk of competing initiatives and actors in an ever-more fragmented domain. This calls for a re-evaluation of traditional protagonists' roles. Particularly as, despite the increasing number of NTAs, traditional state actors continue to be critical agents in CSCB (Eggenschwiler, 2019). Given the interconnected nature of cyberspace, states that pursue their traditional roles as "standard-setters and enforcers of norms" (Eggenschwiler, 2019, p.1) are particularly vital.

States need to value the contributions of NTAs, enabling them to harness their expertise and impulses for CSCB. This can include potential roles for traditional actors as sparring partners of non-traditional actors and initiatives (Eggenschwiler, 2019). While all actors have to take responsibility for their cyberspace activities, notably traditional regulators appear somewhat disconnected from new technologies. Self-regulation and contributions by NTAs can strengthen rules that ensure the future development of the digital economy and information society. If, however, traditional and non-traditional actors are likewise included. Recognising that politics are inevitable in cyberspace is just as crucial as a sensitivity for the debated presumption that a strong regulation could actually stifle innovation and development (Stadnik, 2018). A strategic focus on both effective domestic coordination and the advancement of international engagement is essential. CSCB, however, still tends to lack "necessary top-level leadership attention and support to seize this opportunity" (Hohmann et al., 2017, p. 5).

How does the Federal Republic of Germany position itself? As translated from German, the German key objective is the „strengthening of bilateral and regional support and cooperation for building and advancing cyber capabilities” (Federal Ministry of the Interior, 2021, p. 123). This includes increased cooperation at all levels to build cybersecurity capacity with international (non-)traditional actors from business, civil society and politics. Additionally, cybersecurity shall be more integrated into digital economy programs and stabilisation measures. This indeed responds to the rising international importance of CSCB and is considered fundamental for unfolding the potentials of digitisation while reducing prevailing vulnerabilities.

The conviction that bi- and multilateral cooperation sustainably increase cybersecurity in partner states drives this ambition. Democratic and normative values and ideals can therewith be anchored worldwide. This is believed to result in a global, overall increase in cybersecurity (Federal Ministry of the Interior, 2021). The federal government’s criteria concerning this aim are establishing CSCB as a topic in international committees and relevant policy documents. This is complemented by an assessment of German engagement in CSCB in the national, EU-, NATO- or global context (Federal Ministry of the Interior, 2021). What is remarkable is the explicit recognition of the beneficial impacts CSCB has on German cybersecurity. The new German Cybersecurity Strategy (2021) describes it as an instrument contributing to achieving the delineated objectives (Federal Ministry of the Interior, 2021).

What are the implications for Germany’s future in the field? Germany is well-positioned to take on a key role in CSCB. While efforts are currently still at an early stage, Germany has a robust international network, thorough experience with capacity-building in other fields, and an advanced ICT ecosystem. A vital asset for German CSCB is the ability to rely on existing expertise and an excellent reputation in diplomatic, development and cybersecurity communities (Hohmann et al., 2017). There is strong advocacy for regional cooperation, multi-stakeholder and multidisciplinary CSCB approaches. This goes in hand with recognising the importance of CSCB for internet governance, as CSCB touches on various areas of this field (APC, 2019).

In sharp contrast to matters of cyberwar, cyber stability provides space for activities of a broad range of (non-)traditional actors. Facing the ever-growing heterogeneity of actors, technical complexity, and the blurred borders between public and private matters, policy-makers are challenged with finding appropriate types of governance for CSCB (Eggenschwiler, 2018). Germany has strong diplomatic relations with states in the global south. If these ties are used, Germany could develop into a true CSCB catalyst by speaking up for investments in ICTs, providing CSCB measures in partner states, and showing support for a resilient multilateral effort (Hohmann et al., 2017).

How can Germany shape the next decade of CSCB? First, funding for CSCB initiatives and partnerships is vital and requires discussion, including the German Bundestag. With the appropriate resources, the improved expertise in cybersecurity and the knowledge and experience in building capacity abroad in other sectors can successfully advance CSCB. These efforts need to keep track of the rising global connectivity. As NTAs are set to further increase in relevance and contribution, it is essential that traditional top-level political leaders in key countries, such as Germany, support their efforts (Hohmann et al., 2017).

Another critical aspect is improved coordination between German government bodies. Currently, both the Federal Ministry for Economic Cooperation, the Federal Office for Information Security (BSI) and the Federal Foreign Office share overlapping mandates (Hohmann et al., 2017). Integration of development and cybersecurity expertise is promising if a common language and joint projects are established (Hameed et al., 2018). This is closely related to the appeal for more engagement in multilateral exchange. The EU CyberNet and its annual conference are a major platform for exchange, connecting different communities engaged in EU-funded CSCB activities (EU CyberNet, 2021). These actors bring various tools, methods, knowledge, and funding ideas to the table. This presents a beneficial format for strengthening the German and international CSCB network and enabling a sufficient exchange of knowledge (Collett & Barmpaliou, 2021). Other examples are the UN OEWG and UN GGE 2021's recommendations on CSCB principles and coordination (Collett & Barmpaliou, 2021).

These are two significant steps for shifting traditional actors from discussing CSCB strategies at immediate inter-service meetings or inter-agency consultations to more institutionalised and inclusive processes. Out of the several parent communities, the community of NTAs in international development is of particular importance. Implementing a closer connection with their various digital projects has been recommended in numerous reports (Collett &

Barmpaliou, 2021). These reports include the EUISS's 'Cyber Capacity Building in Ten Points' (Pawlak, 2014a), the World Bank's 'Digital Dividends' (World Bank Group, 2016), and NUPI's 'Teach a Person How to Surf: Cyber Security as Development Assistance' (Schia, 2016).

Due to the increasingly complex CSCB ecosystem, it is essential for Germany, as a current and potential donor country, to evaluate CSCB activities carefully. This helps to assess if existing initiatives can keep up and live up to their potential. Only if existing gaps are discovered they can be future-proofed effectively (Collett & Barmpaliou, 2021). Addressing gaps includes openness to NTAs and specialists. Achieving this may include increased consultation of cybersecurity professionals from other traditional government bodies or institutional investment in *cyber knowledge brokers* across all levels (Pawlak & Barmpaliou, 2017). Most importantly, it means improving external experts' involvement in creating new initiatives (Collett & Barmpaliou, 2021).

Multi-stakeholder processes can be best suited for advancing the rapidly increasing range of non-traditional and traditional actors. A principle-based approach to security capacity building in cyberspace is the basis for providing an outlook towards sustainably closing current capacity gaps. Such strategies include (non-)traditional organisations and single (partner) states alike, with a common aim to advance the global CSCB ecosystem (Dutton, 2015). Finally, countries like Germany, with strong experiences with various multilateral formats, seem to be better positioned to pioneer new multilateral approaches (Kortunov, 2020). The ongoing cross-thematic German discourse on multilateralism is essential and timely for future CSCB.

In sum, these factors indicate that Germany is in an excellent position to take on a vital role in the field of CSCB in the future, even as its related efforts are still at an early stage now.