FACULTY OF POLITICAL AND SOCIAL SCIENCES

International Development in the Field of Cybersecurity:

The EU's role between geopolitical encounters and a human-centric digital transformation

Word count: 23,959

Leoni Papritz

Supervisor: Prof. Dr. Jan Orbie

Master's dissertation submitted in order to obtain the academic degree of Master of Arts in Global Studies

Academic year: 2023/2024

GHENT UNIVERSITY

Abstract

This thesis explores the role of the European Union (EU) as a global actor in the domain of cybersecurity and cyber capacity building (CCB). It integrates perspectives from international development, cyber governance, international cybersecurity, and the EU's global actorness to analyse how the EU portrays cybersecurity, capacity building, and its role as a global development actor. By utilising frame analysis, the study assesses the EU's strategic global frameworks, cyber diplomacy, international cybersecurity and CCB documents.

The research highlights that the EU uses a multifaceted approach in its framing, intertwining external and internal security, normative values, growth, and geopolitical concerns. This signifies the importance the EU places on cybersecurity for both global and European stability and prosperity. While the EU strongly advocates for a human-centric digital transformation that is based on an idealist approach and fundamental rights, my analysis shows that its initiatives are also influenced by strategic and geopolitical considerations. Eurocentric perspectives and (post)colonial imaginaries of power create this dual narrative together with the EU's goal to carve out a unique identity in a changing world order through technology and cyberspace. My thesis critically examines the EU's endeavours to promote global cybersecurity development, revealing tensions between the EU's normative goals and its rising strategic interests, highlighting the influence of colonial power structures, and identifying risks of perpetuating global inequalities despite the EU's emphasis on equal partnerships. The research contributes to the literature on international cybersecurity, international development, and EU external relations, providing insights into the complexities of the EU's position in the global digital arena.

Key words: cyber capacity building, EU as a global actor, cybersecurity, international development, geopolitics, human-centric digital transformation.

A comment on the vocabulary: There are various labels and terminologies, e.g. 'net,' 'e-,' 'digital,' etc. I decided to stick with the term 'cyber-' in particular, as this is used by the EU and the academic literature I am referencing. However, I am aware of the critical debate surrounding this terminology, especially in relation to the mystification of 'cyber.'

Table of Contents

List of Abbreviations

ABBREVIATION	EXPLANATION
ACP	African, Caribbean and Pacific Group of States
CBM	Confidence-building measures
CCB	Cyber Capacity Building
CERT	Computer Emergency Response Team
CS	Cybersecurity
CSIRT	Computer Security Incident Response Team
CSO	Civil Society Organisation
DCAF	Geneva Centre for Security Sector Governance
DG CNECT	Directorate-General for Communications Networks, Content and Technology
DG HOME	Directorate-General for Migration and Home Affairs
DG INTPA	Directorate-General for International Partnerships
DG NEAR	Directorate-General for Neighbourhood and Enlargement Negotiations
DSM	Digital Single Market
EDF	European Development Fund
ENISA	European Network and Information Security Agency (EU)
EPRS	European Parliamentary Research Service (EU)
EU	European Union
EUISS	EU Institute for Security Studies
FPI	Foreign Policy Instrument (EU)
GCCS	Global Conference on CyberSpace
GDPR	General Data Protection Regulation (EU)
GFCE	Global Forum on Cyber Expertise
GPPI	Global Public Policy Institute
ICT	Information and Communications Technology
IGF	Internet Governance Forum (UN)
IT	Information Technology
ITU	International Telecommunication Union (UN)
NATO	North Atlantic Treaty Organisation
NDICI	Neighbourhood, Development and International Cooperation Instrument – Global Europe (EU)
NGO	Non-Governmental Organisation
NSA	National Security Agency (United States)
NUPI	Norwegian Institute of International Affairs
OEWG	Open-Ended Working Group (UN)
SDG	Sustainable Development Goals
UN	United Nations
UN GGE	UN Group of Governmental Experts on Developments in the Field of ICT in the Context of International Security
RUSI	The Royal United Services Institute for Defence and Security Studies (UK)
WSIS	World Summit on the Information Society (ITU)

1. Introduction

Cybersecurity has become a critical issue in global politics, as evidenced by numerous instances that have come to light in recent years. These include attacks on Estonian e-Government services in 2007, the Snowden revelations in 2013 which uncovered major international wiretapping activities by the NSA, Russian hacker groups involvement in the Hilary Clinton election campaign in 2016, numerous cryptocurrency frauds and data thefts, ransomware attacks by groups like Wannacry, the role of cyberattacks and espionage in conflicts from Ukraine to Iran, and TikTok as a topic of heated debate in global politics – the list is endless.[1] These events highlight the ubiquity of cyber threats and their potential global impact.

Cyberattacks target sensitive data of individuals, the sovereignty of national governments or even cross-border processes, with ordinary people remaining the most vulnerable victims.[2] And the significance of these issues only continues to grow as our personal and professional lives become increasingly reliant on digital networks and technology, making cyber-related threats "one of the greatest global risks now."[3] However, not all regions and countries are considered to have equal resources and infrastructure to address these threats. This is where international development actors come into play, which aim to address digital inequalities and call for cyber capacity building to enhance cybersecurity, resilience, and digital skills worldwide. However, the geopolitical landscape, both in the Global North and in the South, plays a crucial role, with Southern countries facing the intersection of competing global interests. This study examines how the EU positions itself as a global development actor in the field of cyber capacity building and how it constructs a European identity through its international cybersecurity development activities.

1.1. A Global Studies Approach to Cybersecurity

Understanding cybersecurity in global politics requires a comprehensive approach to cyber capacity building. The field of Global Studies provides a suitable framework, recognising the interconnectedness of the local and global and rejecting binary, Western-

[1] Deibert, 'Cyber-Security', 324–25; Kerttunen and Eneken, 'The Politics of Stability. Cement and Change in Cyber Affairs', 61; Chiappetta, 'The Cybersecurity Impacts on Geopolitics', 61–63.
[2] Chiappetta, 'The Cybersecurity Impacts on Geopolitics', 65.
[3] Chiappetta, 67.

centric thinking. This perspective enables a more nuanced understanding of global entanglements, critical perspectives on technology and development, and challenges conventional wisdoms and flawed assumptions. The Global Studies approach is informed by a historicised and postcolonial angle and will shape the conceptual framework and methodology of this thesis.[4] While the Internet and technological advancements may seem global, it is important to note that there is no single, unified digital space that is inherently global. It is shaped by both local and international actors, and power dynamics are present within it, which is why the Internet and digital technologies are always in an intertwined process of becoming globalised and deglobalised.

In the postcolonial approach, there are a few key concepts that shape the analytical perspective. One such concept is the coloniality of power (colonialidad de poder) by the Peruvian sociologist Aníbal Quijano.[5] It refers to the ongoing continuation of colonial power structures beyond the formal existence of the colonies, maintaining the relationship between the coloniser and colonised. This dynamic perpetuates the remnants of colonial times, referred to as the colonial legacy, and is evident in the core of the global capitalist system. Quijano argues that this system is Eurocentric and based on the exploitation of racialised people from former colonies.[6] Furthermore, it influences European foreign and development policy until today through knowledge production and discursive power.[7]

The European Age of Enlightenment established a Eurocentric worldview,[8] which positions Europe (or the West) as the focal point of history, modernity and knowledge, while deeming the rest of the world as backward, traditional and irrational. This results in the non-West being constructed as the 'Other,' as famously analysed by Edward Said in his pivotal work, *Orientalism*.[9] The Eurocentric worldview underpins the way we think about history, geography and innovations. This perspective shapes our understanding of empirical reality and suggests that the most influential political and social concepts, such as democracy, the nation-state, peace, progress, science and technology, originated from the

[4] Middell, 'What Is Global Studies All About?'; Darian-Smith and McCarty, 'Why Is Global Studies Important?'
[5] Quijano, 'Colonialidad del poder, Eurocentrismo y América Latina'.
[6] Quijano, 208.
[7] Sebhatu, 'Applying Postcolonial Approaches to Studies of Africa-EU Relations', 40–42.
[8] Unwin, 'Development Agendas and the Place of ICTs', 8.
[9] Said, *Orientalism*.

pens and minds of clever Europeans. However, postcolonial historians argue that this is a distortion of reality. Eurocentrism is deeply ingrained in the European intellectual understanding of society and has been used to justify Europe's actions around the world for centuries. It was instrumental to maintain power and wealth gained through colonisation and exploitation, continuing into the postcolonial period of history.[10]

The main objective of Global Studies is to shift focus away from Europe as the centre and instead view it from a decentred or provincialised perspective. I adopt this analytical approach because it strives to reevaluate Europe's role in its relationship with the non-European so-called developing countries, and to challenge the notion that Europe has been more important to Africa than vice versa. By examining historical narratives and deconstructing the idea of the EU as a global development actor, this approach seeks to question traditional discourses and bring attention to colonial continuities in how the EU imagines itself as a global player in a multipolar world order.[11] This perspective informs my approach to EU international development in the field of cybersecurity, conceptualised as cyber capacity building.

1.2. International Development and the Role of Technology

The roots of development can be traced back to the period of decolonisation after World War II. Former colonies were gaining independence, but power and influence continued to be asserted in a different, more subtle way. The 'colonies' turned into 'underdeveloped countries' or the 'third world.' This transformation gave rise to the concept of 'development.' It morphed the colonial European 'superiority' over racialised peoples into an integrated, institutionalised system. The objective now was to bring about social and political change, fight poverty, and integrate these countries into the world economy. The same ideological foundation emerged in new disguise. A whole development 'industry' evolved, including a wide range of international organisations, research institutes, governmental and non-governmental agencies.[12]

[10] Blaut, *The Colonizer's Model of the World: Geographic Diffusionism and Eurocentric History.*, 9–10; Sebhatu, 'Applying Postcolonial Approaches to Studies of Africa-EU Relations', 40–43.
[11] Orbie, 'The Graduation of EU Development Studies', 599; Sebhatu, 'Applying Postcolonial Approaches to Studies of Africa-EU Relations', 43.
[12] Cooper and Packard, 'Introduction', 1–2.

Technology has always played a significant role in development. It is important to reconsider the understanding of technology in development, which tends to be Eurocentric and diffusionist. This perspective views technology as originating in the West and then being introduced to the 'developing world' for positive change. This creates a dynamic of 'centre' and 'periphery,' with innovations supposedly flowing from the West to the rest of the world.[13] European-centred technology, from mining to 'conventional' medicine, has often been portrayed as 'heroic' and has reinforced global dependencies and hierarchies.[14]

The 20th century saw a shift in global leadership in innovation and progress. It became clear that the United States were surpassing Europe as the pacesetter in technological developments. This switch impacted not only Europe itself, but also its colonies and former colonies. European technological dominance slipped away.[15] Pioneering technological inventions such as the Internet, mobile phones and computers, social media platforms like Instagram and WhatsApp, as well as recent advancements in blockchain technology and artificial intelligence, predominantly originate in the United States.

Despite the EU falling behind in technology, and development policies changing over time, technology continues to be a key element in development. Digitisation has become a fundamental component of various EU policy initiatives, including development and neighbourhood policies. While in the 20th century, development focused on building physical infrastructure such as dams, bridges, or highways, in the 21st century, development efforts also incorporate digital technology. Cyber capacity building (CCB) is a particularly timely area of international cooperation concerning cyber-related issues, focusing on bolstering digital infrastructure against cyberattacks, improving digital skills, or developing secure e-government services.

Digital technology is an issue of our daily life; but it also affects international relations, power dynamics, and security concerns. The shift from traditional to digital infrastructure and capabilities mark a new era in geopolitics, which now includes information flows, cybersecurity, and digital innovations. So, how does geopolitics come to play here?

[13] Blaut, *The Colonizer's Model of the World: Geographic Diffusionism and Eurocentric History.*, 11–12.
[14] Arnold, 'Europe, Technology, and Colonialism in the 20th Century', 89.
[15] Arnold, 90.

1.3. Geopolitics in Transition: Colonial Legacies and Cyberfrontiers

Geopolitics, what it means and what it can offer, is widely discussed. In its definition, geopolitics refers to how states compete for control and influence over territory. The idea of geopolitics has its roots in Western imperial thinking about global affairs and projects a particular understanding of geography and politics to delineate ideological and cultural distinctions.[16] Imperial geopolitical thinking manifests itself in rhetoric like "'the spread of free markets' or the 'diffusion of democracy.'"[17] Already the division between the 'developed' Global North and the 'underdeveloped' Global South is shaping a "geopolitical reality."[18]

An example for geopolitics in practice is the "Scramble for Africa." The term refers to the competition among European powers to divide and control African land and resources.[19] In the 1950s, during the Cold War, Africa once again became a disputed territory for geopolitical competition and a proxy venue for the rivalry between the US and the Soviet Union.[20] Today, Africa is "reemerging as a key space of interest in the geopolitics of globalization, with the EU, China, the United States and others scrambling for control over Africa's vast natural resources and emerging markets."[21]

The digital sphere is becoming increasingly relevant for geopolitics. International actors start to contest for digital territories, build strategic alliances, and assume competing roles. While Europe may not be as innovative as the US and China, it is positioning itself as a regulator and a normative power. It advocates for a "human-centric digital transformation" and places data protection, privacy, and the ethical use of technology at the heart of its agenda. The EU thereby aims to distinguish itself from other global players as the 'good' or 'soft power' and "emerge as a separate 'pole' for a multipolar world order,"[22] while aiming to address US hegemony, dependency on Chinese production, and the

[16] Kumar, *Geopolitics in the Era of Globalisation. Mapping an Alternative Global Future*, 7–8.
[17] Flint, *Introduction to Geopolitics*, 16.
[18] De Roeck, Delputte, and Orbie, 'Framing the Climate-Development Nexus in the European Union', 10.
[19] Flint, *Introduction to Geopolitics*, 13.
[20] Hansen and Jonsson, 'Bringing Africa as a "Dowry to Europe"', 461.
[21] Hansen and Jonsson, 461.
[22] Kumar, *Geopolitics in the Era of Globalisation. Mapping an Alternative Global Future*, 44.

influence of authoritarian regimes.[23] However, the effectiveness of this strategy hinges on the EU's ability to garner widespread support outside its borders, including from countries in the Global South.

Despite the historical baggage of colonialism, both the EU and the US seem to rely on their deep historical and cultural ties when engaging with the countries in the Global South. However, historical grievances often taint present-day relationships, leading many nations to approach Western partnerships with scepticism. They are wary of potential neocolonial undertones and new forms of digital colonialism and are dissatisfied with being seen as mere recipients of development initiatives, rather than equal partners. Instead, many countries turn to China and Russia as their alternative partners. These partnerships are appealing because they come with less historical baggage and fewer conditions, allowing recipient countries to pursue their development goals more independently.[24]

Additionally, the relationship between geopolitics and cybercrime has become increasingly intertwined. Hacking, espionage and digital interference are now being used as tools by states to exert influence and power on the international stage. Especially for larger powers, cyberspace is becoming a strategic tool, and in some cases, a weapon. It is an environment that is increasingly integrated into the political, geopolitical, and military sphere, a source of tension and competition.[25] Geopolitics is also being debated more intensely in the EU context, and I integrate it into my analysis as an angle to examine the EU as a global actor.

In her trenchant paper, *Interrogating the Cybersecurity Development Agenda: A critical reflection*, Louise Marie Hurel (2022) invites a broader and more in-depth exploration of literature on cybersecurity in the context of development. Hurel emphasises the importance of adopting a critical, reflective perspective and addressing the marginalisation of the Global South in cybersecurity development. I agree with her perspective and intend

[23] Fritzsche and Spoiala, 'The EU-AU Digital Partnership', 5; Erforth and Martin-Shields, 'Where Privacy Meets Politics: EU-Kenya Cooperation in Data Protection', 142; Fritzsche and Spoiala, 'The EU-AU Digital Partnership', 24.
[24] Izycki, Van Niekerk, and Ramluckan, 'Cyber Diplomacy', 416–24; Fritzsche and Spoiala, 'The EU-AU Digital Partnership', 17.
[25] Chiappetta, 'The Cybersecurity Impacts on Geopolitics', 71.

to further contribute to this approach by critically examining the EU's role as a global actor in cybersecurity development – an aspect that has not been sufficiently addressed in the literature so far.

1.4. Problem Statement and Research Questions

In recent years, the European Union has been increasingly integrating digital transformation into its policy initiatives and activities, including international partnerships and development policy. Historically, international development can be interpreted as the continuation of postcolonial power dynamics, with the West explicitly or implicitly positioning itself as an advanced, superior provider of technology and knowledge, catering to a Eurocentric paradigm. In the past decades, a lot has changed in rhetoric, practices and world order. However, these dynamics are persistent even in contemporary approaches to development, including digital development. In contrast to other global powers, the EU positions itself as a regulator and normative power advocating for a human-centric digital transformation and trying to advance European norms and values internationally through cyber capacity building.

However, while the EU presents its global digital initiatives as grounded in normative aspirations concerning democracy, human rights, and the rule of law, it remains unclear to what extent these efforts are influenced by underlying geopolitical strategies and security concerns. This study hypothesises that while the EU emphasises normative, human-centric values in its international digital development rhetoric, its cybersecurity and cyber capacity building efforts are likewise significantly motivated by geopolitical interests, reflecting a strategic approach to global cyber governance.

This thesis investigates the role of the EU as a global actor in cybersecurity development. I argue that the colonial legacy of the EU's position as a global actor in continues to influence the field of cyberspace and digital technologies today. By analysing the EU's framing of cybersecurity and its cyber capacity building initiatives, this research will contribute to filling the literature gap of the EU as a global actor in CCB and critically analyse the EU in its most contemporary form of being a development actor.

To explore the issue, the following research question has been developed:

How does the EU frame the cybersecurity domain and its contribution to cybersecurity and cyber capacity building?

The focus of the question is on the EU as the central actor, with an analytical focus on framing and a thematic focus to the EU's perception of international cybersecurity and its role in cyber capacity building. The main research question is supported by sub-questions to clarify the process. The first sub-question is based on the critical, and historically informed perceptions that are essential in Global Studies:

To what extent does the EU's role as a global digital actor in cybersecurity and cyber capacity building rely on postcolonial structures and Eurocentric ideologies?

Based on the explorative research I have conducted on the EU and its digital development activities, I have developed a second sub-question. It centres around the EU's dual role as a soft power with a normative, human-centric approach, as well as a geopolitical power with strategic interests. This sub-question will help to assess this positioning.

How does the EU balance its commitments to an idealistic, human-centric digital transformation with potential realist, geopolitical, and strategic interests?

In answering these questions, I will proceed as follows: First, the background chapter offers contextual information on international and EU cybersecurity efforts as well as processes and institutions of cyber capacity building. The theoretical framework provides theoretical context for my research case in the fields of international development, cyber governance, international cybersecurity and the EU as a global digital actor. In the literature study, I examine existing literature on CCB, looking at characterisations, tensions and political aspects. The methodology chapter elaborates on my research design and the primary methodological tool, frame analysis. Next, I give a detailed analysis of the EU's framing of itself as a global actor and of cybersecurity and CCB based on the analysed documents. Following that, I discuss and interpret the findings, highlighting the implications for the EU's role as a global actor in cybersecurity development. Finally, I summarise my main findings and present concluding remarks.

2. The Evolution of Cybersecurity and Capacity Building Policies

The first United Nations resolution on cybersecurity was adopted in 1999, marking a pivotal moment for the multilateral approach to cybersecurity governance.[26] In the early 2000s, cyber capacity building emerged on international agendas. International organisations like the International Telecommunication Union (ITU) and NATO included capacity building for the use of ICTs in their mandates and reports.[27] The ITU World Summit on the Information Society (WSIS) took place in 2003 in Geneva and in 2005 in Tunis, resulting in a joint declaration and agenda for developing an Information Society and placing cybersecurity and cyber governance on international political agendas.[28] In 2015, the WSIS+10 meeting took place in New York and called for a better connection of Global South countries and the integration of ICTs into the Sustainable Development Goals (SDGs).[29]

Despite making a start, it took several years for CCB to take off. Only in the 2010s did projects start to exceed more than ten per year. While CCB has grown continuously, it has received relatively little attention and financing compared to other fields in the international development community.[30] One challenge is that CCB projects are interdisciplinary and bring together various parent communities. However, these communities tend to operate in silos, creating barriers that require considerable time and effort to overcome.[31]

In recent years, actions have been taken to prevent further patchwork and fragmentation in CCB. The Global Forum on Cyber Expertise (GFCE) is a prominent platform where multistakeholder actors from various disciplines come together to discuss best practices and the future of CCB. The GFCE was established in 2015 at the Global Conference on

[26] Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South', 823.
[27] Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 300.
[28] Sund, 'Towards an International Road-map for Cybersecurity', 567.
[29] Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South', 823.
[30] Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 300.
[31] Pawlak and Barmpaliou, 'Politics of Cybersecurity Capacity Building', 131–32.

CyberSpace (GCCS) in The Hague and has since advanced multiple projects and coordination efforts worldwide.[32]

Two important institutions at the UN are the UN Group of Governmental Experts on Developments in the Field of ICT in the Context of International Security (GGE) and the Open-Ended Working Group (OEWG). Both groups examine emerging threats, confidence and capacity building, international law for ICTs, and responsible state behaviour in cyberspace to produce reports, recommendations and conclusions for the UN General Assembly. There was a total of six GGEs which operated between 2004 and 2021. The OEWG was established in December 2018 and operated until 2021 in a multistakeholder setting, including industry, civil society, and academia.[33]

A significant legal instrument for global cybersecurity is the Council of Europe's *Budapest Convention on Cybercrime*. This convention facilitates international cooperation in combating cybercrime and has been ratified by countries both inside and outside of Europe.[34] However, neither China nor Russia ratified it.[35] The NATO *Tallinn Manual on the International Law Applicable to Cyber Warfare* provides guidance on how existing international law applies to cyber operations.[36]

Over the past 20 years, the EU has made efforts to establish itself as a digital actor and enhance its cyber capacities. The European development of a cybersecurity policy began in the 1990s.[37] In 2004, the European Network and Information Security Agency (ENISA) was established.[38] The cyberattacks on Estonian e-government services in 2007 caused widespread concern and prompted the EU to demand action plans and improved cybersecurity measures from its member states. This attention led to several new digital projects and developments, including the Digital Single Market (DSM), the European Cybercrime Centre, and Computer Emergency Response Teams (CERTs).[39] CERTs,

[32] Kurbalija, *An Introduction to Internet Governance*, 86; Pawlak and Barmpaliou, 'Politics of Cybersecurity Capacity Building', 125–26.
[33] United Nations Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the Context of International Security'.
[34] Kurbalija, *An Introduction to Internet Governance*, 87.
[35] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185'.
[36] Kurbalija, *An Introduction to Internet Governance*, 92.
[37] Renda, 'The Development of EU Cybersecurity Policy', 489.
[38] European Union Agency for Cybersecurity, 'About ENISA - The European Union Agency for Cybersecurity'.
[39] Renda, 'The Development of EU Cybersecurity Policy', 476–78.

sometimes referred to as Computer Security Incident Response Teams (CSIRTs), play a crucial role in CCB initiatives to improve and coordinate cybersecurity efforts.[40]

The EU has published three cybersecurity strategies so far. In 2013, the EU introduced its first Cybersecurity Strategy under the motto "open, safe and secure cyberspace."[41] Since the 2013 Strategy, there has been a growing awareness of international cyber capacity building.[42] It was followed by the 2017 Cybersecurity Strategy.[43] The most recent strategy, the Cybersecurity Act published in 2020,[44] focuses on addressing growing cybersecurity threats posed by increased geopolitical tensions and once again emphasises the EU's commitments to preserving an open and free cyberspace based on European values.[45]

The most prominent success for the EU so far in digital policy was the adoption of the General Data Protection Regulation (GDPR) in 2016.[46] This gave rise to the term 'Brussels Effect' coined by Anu Bradford. The 'Brussels Effect' refers to the potential phenomenon where the EU's legislation influences global policy developments and sets new standards.[47] While the actual regulatory influence of the GDPR on data protection and privacy worldwide cannot be adequately measured, some preliminary studies suggest that it had global influence at least to some extent, leading to the GDPR being seen as a "global gold standard."[48]

For the EU, cyber capacity building is a relatively new area of international cooperation. A mapping of EU-funded CCB activities in 2022 gives insights into the EU's initiatives in the field. Key actors involved on the EU's side include the EU Cyber Capacity Building Network (EU CyberNet), the Service for Foreign Policy Instruments (FPI) of the European Commission, and the European External Action Service (EEAS). Involved departments within the Commission are the Directorate-Generals for International Partnerships

[40] Kurbalija, *An Introduction to Internet Governance*, 88–89.
[41] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'.
[42] Amazouz, 'Cyber Capacity-Building and International Security', 205.
[43] European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU'.
[44] European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade'.
[45] Renda, 'The Development of EU Cybersecurity Policy', 469–85.
[46] Creese et al., 'The Solution Is in the Details', 2.
[47] Mărcuț, 'Evaluating the EU's Role as a Global Actor in the Digital Space', 79.
[48] Cervi, 'Why and How Does the EU Rule Global Digital Policy', 2–6.

(DG INTPA), for Neighbourhood and Enlargement Negotiations (DG NEAR), for Communications Networks, Content and Technology (DG CNECT), and for Migration and Home Affairs (DG HOME).

The report mapped a total of 33 CCB actions with an overall funding of €178.95 million, categorised into the four primary focus areas: cybersecurity (€65.35 million), cybercrime (€54.43 million), cyber diplomacy (€3.50 million), and mixed actions (€55.67 million). The financial instruments involved are the Global Europe: Neighbourhood, Development and International Cooperation Instrument (NDICI), as well as the Instrument contributing to Stability and Peace (IcSP), the European Neighbourhood Initiative (ENI), and the European Development Fund (EDF).

Geographically, the EU's CCB initiatives cover global, regional, and country-specific scopes. Six actions operate on a global level, 18 have a regional focus, and nine are country specific. Key regions receiving support include the Eastern Neighbourhood (11 actions), Sub-Saharan Africa (9 actions), the Western Balkans (7 actions), the Asia-Pacific region (7 actions), Latin America and the Caribbean (5 actions), and the Southern Neighbourhood (4 actions).[49]

3. Theoretical Framework

Before delving deeper into the concept and relevance of cyber capacity building, I embed the EU and its global CCB activities in theoretical fields related to my research focus: international development, cyber governance, international cybersecurity, and the EU's global actorness.

3.1. International Development

This chapter examines the concept of international development and EU development policy from a postcolonial perspective, highlighting how historical legacies and Eurocentric ideologies continue to shape contemporary practices and discourses.

To understand the roots of the EU's international development, it is necessary to have a look back in time. The ideological roots of European integration can be traced back to

[49] EU CyberNet, 'Mapping of EU-Funded External Cyber Capacity Building Actions 2022', 3–6.

Interwar period and, among other strategic reasons, stemmed from the desire to retain control over Africa. During this time, the United States and the Soviet Union were gaining economic and political power, which prompted European states to maintaining its economic and geopolitical position through the Eurafrican idea. Africa was seen as a provider of natural resources, agricultural products, raw materials, hydroelectric energy, and potential living space for the European population.[50]

The Treaty of Rome negotiations then marked the official beginning of the history of the European integration project, which ultimately led to the founding of the European Union. The Rome negotiations took place in the mid-1950s and resulted in the establishment of the European Economic Community (EEC). The colonial possessions quickly came to play a central role. France successfully pushed for the inclusion of l'Algérie française and all other colonial territories of European member states into the EEC, ranging from Belgian Congo to Netherlands New Guinea. The aim was to maintain close ties and shape the further development of these territories. This led to the establishment of the European Development Fund (EDF), which is still active today.[51] The integration of mainly French and Belgian colonies began with the EDF and was maintained throughout the Yaoundé Conventions (1964-75) as well as the Lomé (1975-2000) and Cotonou (2000-2020) Agreements. The first configuration of target countries came to be known as the Africa Caribbean Pacific (ACP) partnership.[52]

Ever since its inauguration, the EU development policy has evolved under historical trends, including the modernisation and dependency theory, neoliberalism, and the influence of the Bretton Woods institutions. Especially since the 1980s, this has faced heavy criticism for contributing to global inequalities, prioritising profit interests, and causing adverse effects on recipient states, such as the debt crisis in Latin America or the food crisis in Africa.[53] By the mid-1990s, this led to a shift from the growth-centred paradigm towards combating poverty and a 'people-centred approach.'[54]

[50] Hansen and Jonsson, 'Bringing Africa as a "Dowry to Europe"', 442–49.
[51] Hansen and Jonsson, 454–55.
[52] Orbie, 'International Development. A Distinct and Challenged Policy Domain', 425.
[53] Mason, *Global Shift. Asia, Africa, and Latin America, 1945-2007*, 260–64.
[54] Doidge and Holland, 'A Chronology of European Union Development Policy: Theory and Change', 68–76.

Currently, the EU is operating within the Post-Cotonou Agreement and aims to streamline and differentiate its policy for the Global South to achieve a better 'global impact.'[55] A particular emphasis is on 'Europeanising' development policy by aligning it with European values and normative aspirations,[56] and on creating 'nexuses,' which connect or overlap areas of different policy domains.[57] The security-development nexus underscores the idea that security is a prerequisite to achieving development objectives, and likewise, development will contribute to establishing global peace and security. However, there is an ongoing debate about whether integrating security into development policy is making development politically more relevant, or if that is overshadowing the original developmental objectives in a "pursuit of a global power Europe."[58]

The concept of capacity building has been prevalent in international development since the end of World War II. Initially, it was a part of public administration,[59] with the idea to 'give' knowledge, expertise and technology, conceptualised as 'technical assistance.' Capacity building then gained prominence as policymakers considered it as "a 'lighter touch' to assistance or 'less political' alternative to more traditional approaches."[60] Five decades later, with the UN Rio Declaration on Environment and Development in 1992, capacity building further neutralised and adopted into the realm of sustainable development.[61] In terms of cybersecurity, capacity building is now considered a central tool to establish a minimum global standard of cybersecurity.[62]

With this brief history of development, it becomes clear that the EU's development policy is deeply rooted in historical colonial relationships.[63] Continuous efforts have been made to portray the EU's international endeavours as being 'interdependent,' 'pioneering' and

[55] Orbie, 'International Development. A Distinct and Challenged Policy Domain', 437.
[56] Orbie, 'The EU's Role in Development: A Full-Fledged Development Actor or Eclipsed by Superpower Temptations?', 23–25.
[57] Delputte and Orbie, 'Paradigm Shift or Reinventing the Wheel?', 244.
[58] Orbie, 'The EU's Role in Development: A Full-Fledged Development Actor or Eclipsed by Superpower Temptations?', 33.
[59] Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 301.
[60] Hurel, 'Interrogating the Cybersecurity Development Agenda: A Critical Reflection', 68.
[61] Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace', 226; Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 301.
[62] Pawlak and Barmpaliou, 'Politics of Cybersecurity Capacity Building', 129.
[63] Doidge and Holland, 'A Chronology of European Union Development Policy: Theory and Change', 60; Orbie, 'International Development. A Distinct and Challenged Policy Domain', 425.

'modernising,' rather than reflective of an exploitative coloniser-colonised relationship.[64] Scholars describe the construction of 'underdevelopment' in Africa and other regions as "historical amnesia" – an ahistorical perspective in which Europe's past colonial presence is conveniently forgotten. "This historical amnesia is co-constitutive of how the EU imagines itself as a global actor and power, 'by […] successfully entrenching the myth of its own 'virgin birth'' (Nicolaïdis 2008, cited in Fisher Onar and Nicolaïdis, 2013:292)."[65]

This is also reflected in language. What used to be called 'development aid' was then referred to as 'development cooperation' and ultimately as 'international cooperation.' In 2021, the European Commission's Directorate-General for Development and Cooperation (DG DEVCO) was renamed to International Partnerships (DG INTPA), highlighting their cooperative approach.[66] However, despite these changes in terminology, postcolonial literature hints at the fact that the practical implementation may not change, and that the concept of development remains problematic due to continuous asymmetric power relations and a lack of recognition of non-Western agency. With this theoretical foundation in mind, I will now discuss cyberspace and its governance as an issue of global politics.

3.2. Cyber Governance

This chapter clarifies key terminology and concepts, introduces cyber governance, and lays the foundation for understanding the EU's approach to cyber governance, navigating between fragmentation and diplomacy.

Understanding terminology is an essential starting point. The most common word is surely 'governance': "Governance ensures that stakeholders' needs, conditions, and options are balanced. It allows a determination of the management and administration in decision-making and prioritisation, as well as a needs assessment to determine common institutional goals."[67] It is a process that brings together diverse, interconnected actors

[64] Hansen and Jonsson, 'Bringing Africa as a "Dowry to Europe"', 457–58.
[65] Sebhatu, 'Applying Postcolonial Approaches to Studies of Africa-EU Relations', 43.
[66] Directorate-General for International Partnerships, 'DG International Cooperation and Development Becomes DG International Partnerships'.
[67] Savaş and Karataş, 'Cyber Governance Studies in Ensuring Cybersecurity', 8.

with conflicting interests to coordinate and cooperate, creating a steering mechanism for social, economic, and political interactions.[68]

In the field of cyber studies, the definition of terms is not as consistent as in political sciences. Here, I use the term 'cyberspace' as a "'global common,' defined as a 'resource domain to which all nations have legal access' (Buck 1998, p. 6) [...] such as the high seas [...]."[69] For Pawlak, cyberspace is "a digital environment (i.e. the internet, telecommunications networks or computer systems) that people use as means to achieve their social, economic or political goals."[70] Therefore, 'cyber governance' can be defined as the multistakeholder management, administration, and collective decision-making for cyberspace. This involves a wide range of actors from different fields such as governments and public administrations, NGOs and civil society organisations (CSOs) as well as the private sector.[71]

I distinguish 'cyber governance' from the recurring term 'internet governance,' which are closely related but have different focuses. Internet governance includes aspects like managing critical Internet resources such as unique Internet addresses; coordinating standardisation and interoperability of Internet protocol design; enforcing intellectual property rights like patents and copyright; ensuring communication rights and individual freedom; and managing data and infrastructure security.[72] Cyber governance focuses more on the integrity of and "participation, transparency and accountability"[73] in cyberspace. It also deals with a broader risk management and the protection of critical infrastructure and information systems from cyber threats. In short, "the importance and necessity of cyber governance is ensuring cybersecurity."[74] Overall, it emphasises the idea that cyber and digital security should be a collective good and a shared responsibility in the international governance of a common cyberspace.[75]

[68] Savaş and Karataş, 13.
[69] Barrinha and Renard, 'Cyber-Diplomacy', 357.
[70] Pawlak, 'Riding the Digital Wave', 6.
[71] Savaş and Karataş, 'Cyber Governance Studies in Ensuring Cybersecurity', 8–14.
[72] DeNardis, 'The Emerging Field of Internet Governance', 556.
[73] Savaş and Karataş, 'Cyber Governance Studies in Ensuring Cybersecurity', 14.
[74] Savaş and Karataş, 7.
[75] Siudak, 'Cybersecurity Discourses and Their Policy Implications', 326.

Even though cyberspace may seem like a technical space, it is rather a social construct, shaped by social imaginaries and situated knowledge.[76] This understanding has been put forward by scholars of international relations who focus on social constructivism and critical perspectives. Traditionally, there has been a strong emphasis on 'technological determinism' in understanding technology in IR. This concept assumes that technology is an "exogenous variable," that drives inevitable change and develops a life of its own.[77] However, from a historicised and critical perspective, cyberspace and technology cannot be taken as a given. They have been shaped and transformed throughout time. Technology is a driver for societal dynamics, but social, political and cultural factors also shape technological developments.[78]

In its original conception, cyberspace is deterritorialised and decoupled from national borders and physical space. However, cyberspace has become an indispensable strategic domain for major powers. International actors seek to establish themselves in a certain role and influence the internet as a political space based on their values, norms, and general interests. In the book *Four Internets*, Kieron O'Hara, Wendy Hall and Vinton Cerf identify four archetypes of the Internet and the operating powers behind them: Silicon Valley's Open Internet, Brussels' Bourgeois Internet, Beijing's Authoritarian Internet, and DC's Commercial Internet. Additionally, Moscow's Spoiler model presents a fifth variation.[79] Due to geopolitical and ideological divides, major powers seek to shape, regulate, and develop the Internet by intervening in physical Internet infrastructure and technology, as well as by controlling network configurations and content filters. Another tactic is to exert power in governance processes with the aim to advance their own conception and vision of how cyberspace should look like. These dynamics ultimately lead to fragmentation – the coexistence of multiple, differing Internets.[80]

The EU's approach to global cyberspace together with the US can be considered as the 'Western view.' The states advocate for a free, human rights-based, and open cyberspace

[76] Dunn Cavelty and Wenger, 'Cyber Security Meets Security Politics', 10.
[77] Marx and Smith, *Does Technology Drive History?: The Dilemma of Technological Determinism*. **Page xi**.
[78] Dunn Cavelty and Wenger, 'Cyber Security Meets Security Politics', 10.
[79] O'Hara, Hall, and Cerf, *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*.
[80] O'Hara, Hall, and Cerf, 9–11; Finnemore and Hollis, 'Constructing Norms for Global Cybersecurity', 459–60.

with a multistakeholder governance model. However, there are still major differences within this Western conception. The US emphasises innovation and has a strong focus on the private market with minimal regulatory intervention, in the Silicon Valley even more so than in the Washington's model.[81] On the other hand, the EU is viewed as a regulator rather than an innovator and seeks to drive forward legislation and regulations in the areas of digital rights, data protection, and information security. The EU has an 'open' approach to cyber governance and digital sovereignty. It aims to create a secure and resilient cyberspace through collective efforts, considering that cyberattacks are perceived as a shared threat that extend beyond state borders and impact more than just the digital sphere. Additionally, the EU is not just concerned with its own domestic regulations and governance, but also aims to contribute to the international development of a normative framework, assuming the role of a 'norm entrepreneur.' [82]

On the other hand, Russia and China promote advance legal regimes to protect themselves from a perceived threat to their political systems and territorial integrity.[83] Russia adopts a 'closed' approach to technological and digital sovereignty, aiming to centralise control and maintain 'territorial integrity' without interference or influence from foreign entities.[84] Similarly, China has taken an anti-Western approach and focuses on maintaining control over its own territory through comprehensive content filters. In recent years, China has even achieved to create a whole separate Internet.[85]

Cyber diplomacy seeks to address these divides, resolve conflicts and manage diverging interests through institutionalised political means, while promoting a shared sense of an international society in cyberspace. This can take place through bilateral or multilateral channels. The EU strongly promotes a multistakeholder approach to Internet and cyber governance, which involves not only state but also non-state actors.[86]

[81] O'Hara, Hall, and Cerf, *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*, 51.
[82] Claessen, 'Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance', 141–52.
[83] Fritzsche and Spoiala, 'The EU-AU Digital Partnership', 19.
[84] Claessen, 'Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance', 148–49.
[85] Deibert, 'Cyber-Security', 320.
[86] Barrinha and Renard, 'Cyber-Diplomacy', 355–56.

An integral part of diplomacy involves cyber norms. When the discussion around governing cyberspace first came up in the late 1990s, Washington and Europe advocated for norms of responsible behaviour rather than formal treaties and agreements. Norms are implicit expectations of appropriate behaviour that exist in all spheres of social life. Similarly, in the context of international relations, norms shape the behaviour of states, such as regarding the use nuclear weapons. In cyberspace, "Western countries saw norms as a vehicle through which they could improve the stability of cyberspace by establishing a series of easily digestible rules based on existing international law, like the cyber equivalent of 'don't litter', and promoting them aggressively."[87] Ultimately, norms seek to influence behaviour through soft power, especially by stigmatising offensive behaviour.

Next to norms, there are two more potential ways to deal with offensive engagement by states in cyberspace: deterrence and entanglement strategies. The deterrence theory originates from nuclear arms control during Cold War and aims to prevent offensive attacks by making them more costly and less beneficial for the offender. Entanglement strategies aim to prevent attacks by creating interdependence between the parties, making harm to others and self-harm inseparable.[88]

In recent years, scholars have observed a drawback in cooperation and principles that have been effective for several decades. Multilateral agreements are no longer sufficient anymore.[89] Grisgby has even proclaimed the "end of cyber norms" due to the failure of the UN GGE 2017 talks, thereby undoing many years of progress. The author concludes that a possible solution could be to turn towards confidence-building measures (CBM) that aim to increase transparency and prevent misunderstandings that could lead to conflict. Nonetheless, the main interest of all major powers remains to avoid cyber conflicts spilling over into the 'physical' world.[90] This brings us to the discussion on international cybersecurity.

[87] Grigsby, 'The End of Cyber Norms', 111.
[88] Craig, Johnson, and Gallop, 'Building Cybersecurity Capacity', 377.
[89] Saran, 'Striving for an International Consensus on Cyber Security', 93–94.
[90] Grigsby, 'The End of Cyber Norms', 113–16.

3.3. International Cybersecurity

This chapter introduces cybersecurity (CS) as an integral element in governing cyberspace. It discusses micro- and macro-level risks and presents an overview of cybersecurity in social science academic literature.

Although there is no universal definition, cybersecurity can be described as "[...] the protection of the information systems that create the cyber environment from attacks to secure confidentiality, integrity and accessibility of the information processed in this environment, the detection of attacks and CS incidents, the activation of reaction mechanisms against these detections and then returning the systems to their state before the CS incident."[91] Cybersecurity basically addresses all threats and attacks that affect or operate through cyberspace.[92] However, various actors and communities have their own political, societal or corporate perspectives on security, which influence how they identify threats, what they consider relevant, and how they engage specific audiences.[93]

Cybercrime, espionage, and cyber warfare are the main categories of threats. Cybercrime typically aims for economic gain and is becoming increasingly sophisticated, professionalised and widespread. Espionage entails accessing classified information, often with the involvement of a state actor. Cyber warfare uses digital tools as a weapon,[94] as seen in Russia's digital attacks on Ukrainian infrastructure following the military attack since 2022.[95] But how is this executed?

Cyber insecurity stems from vulnerabilities in ICTs. Attackers exploit these vulnerabilities to gain unauthorised access to ICT systems using different methods. *Hacking* is a well-known term that involves obtaining illegitimate remote access and control of an ICT system. A *supply chain attack* aims to infiltrate the original code through a 'back door' with harmful elements. The *Distributed Denial of Service (DDoS) attack* occurs when a website's server is overloaded with artificially generated data traffic, for example by bots,

[91] Bakanlıgı, "National Cyber Security Strategy and 2013–2014 Action Plan. Information Technologies and Communication Authority." Quoted from Savaş and Karataş, 'Cyber Governance Studies in Ensuring Cybersecurity', 11.
[92] Deibert, 'Cyber-Security', 315.
[93] Siudak, 'Cybersecurity Discourses and Their Policy Implications', 322.
[94] Deibert, 'Cyber-Security', 323–25.
[95] Przetacznik and Tarpova, 'Russia's War on Ukraine: Timeline of Cyber-Attacks'.

so that it is no longer able to process any data. The *proximity access* allows the adversary to connect to a nearby network, while the *insider access* involves the disclosure of information by legitimate insiders like Edward Snowden, or illegitimate insiders who gained unauthorised access. These attacks compromise the confidentiality of data, the integrity and usability of ICTs, or result in an overall loss of availability to the ICT.[96]

Cyber-attacks can be carried out by a wide range of actors with different backgrounds and motivations. Hacktivism is conducted by individuals or groups with specific political objectives, such as the collective *Anonymous*. In contrast, individual non-political hackers may have very diverse psychological motives behind their action, including a sense of power and control, personal validation, or thrill. Professional cybercriminals are often organised in groups that operate globally and primarily target financial gains.[97]

States are also major players in cyber activities, using cyber tools for intelligence gathering and military operations.[98] Cyber tools offer advantages over traditional diplomatic or military tools. These include discreetness, anonymity, plausible deniability, also known as the attribution problem, as well as relatively low acquisition and maintenance costs, which makes them accessible even to small states. Additionally, cyber tools are not unambiguous in their application, as their use depends on the intentions of the user. This makes them challenging to control or manage compared to other weapons, like nuclear arms.[99]

In academic literature, cybersecurity is conceptualised in different ways. In traditional security studies, particularly in the realist strand, cybersecurity is considered a factor of state security, with threats usually coming from external sources. In critical security studies, where the term security is defined more widely, cybersecurity is a concern for human security and includes non-state actors and non-military threats.[100] In recent years, there has been an increase in critical reflection within cybersecurity scholarship.[101] Just as other issues, cybersecurity and related studies can be analysed through a postcolonial, race-

[96] Finnemore and Hollis, 'Constructing Norms for Global Cybersecurity', 432–33.
[97] Finnemore and Hollis, 434–35.
[98] Finnemore and Hollis, 434–35.
[99] Grigsby, 'The End of Cyber Norms', 111; Finnemore and Hollis, 'Constructing Norms for Global Cybersecurity', 435.
[100] Calderaro and Craig, 'Transnational Governance of Cybersecurity', 920.
[101] Dwyer et al., 'What Can a Critical Cybersecurity Do?'

sensitive, and feminist lens to uncover epistemic hierarchies and their consequences for the CS community and the end-users.[102] Critics argue that cybersecurity has traditionally been approached from a purely technical perspective, neglecting the expertise and perspectives of individuals who lack access, resources and the type of knowledge considered relevant in the field.[103]

A recurring issue of academic discussion is the securitisation of cyberspace. Cybersecurity, that is information and network security, has increasingly become an object of security concern tied to the security of a political regime.[104] For instance, in 2014, the Chinese President XI reiterated how cybersecurity is a central part of national security.[105] The process of securitisation always revolves around an external threat with a specific target, which Siudak calls "threat politics."[106] The lingering danger of this (potential) threat is used to legitimise the government's adoption of specific measures for protection. As a result, many countries have prioritised military capabilities and strategies.[107] This has raised concerns that cybersecurity is being used to justify mass surveillance, exploitable vulnerabilities in ICTs by default, the development of spyware, and expanded privileges for law enforcement privileges to combat 'terror' or 'cybercrime.' This makes civil society critics increasingly worried about the erosion of fundamental rights and civil liberties.[108] This chapter has indicated that cybersecurity is inherently linked to power and political interests.

3.4. The EU as a Global Actor in Cyberspace?

In this chapter, I examine the case of the EU in cyberspace and the debate around its actorness and global power, laying the groundwork for exploring its eternal search for a 'European identity.'

[102] Mumford and Shires, 'Toward a Decolonial Cybersecurity'.
[103] Dwyer et al., 'What Can a Critical Cybersecurity Do?', 2–3.
[104] Claessen, 'Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance', 144; Deibert, 'Cyber-Security', 315; Dunn Cavelty, 'Cybersecurity between Hypersecuritization and Technological Routine', 11; Hurel, 'Interrogating the Cybersecurity Development Agenda: A Critical Reflection', 70–71.
[105] Chiappetta, 'The Cybersecurity Impacts on Geopolitics', 65.
[106] Siudak, 'Cybersecurity Discourses and Their Policy Implications', 327.
[107] Hurel, 'Interrogating the Cybersecurity Development Agenda: A Critical Reflection', 70.
[108] Deibert, 'Cyber-Security', 316.

Cyber power is essentially the capability to mobilise cyber-related resources to achieve specific objectives within, or outside of, cyberspace.[109] The most powerful resource in cyberspace is the access to and availability of information, which is created, transferred, and exploited using ICTs.[110] In this context, the EU has sought to use this strategic opportunity and establish itself as an international actor and a global player in cyberspace.[111]

The legislative foundation for the EU to become an international actor was set with the 2009 Treaty of Lisbon.[112] The treaty enabled the EU to sign international treaties, engage in international relations and actively participate in global digital affairs. It introduced the EEAS, led by the High Representative for Foreign Affairs, which serves as the EU's diplomatic institution. Since then, the EU has gained international acknowledgement, both de facto and de jure, and regulatory authority in digital policy.[113] The EU Global Strategy (EUGS),[114] published in 2016, is a strategic framework which aims to increase the EU's global coherence in the strategy, security and defence fields. It seeks to better integrate the EU's internal and external security strategies and has incorporated cybersecurity into the global strategy.[115]

Internationally, the EU aims to offer an alternative approach to digital cooperation, especially for African partners. It positions itself as a counterpart to US and Chinese-led models[116] by advocating a 'human-centric' model of digital transformation.[117] This strategy hinges on the construction of an 'ontological Other,' where primarily China is seen as an economic competitor and geopolitical rival in the economic and technological sector, posing a security threat to European standards, infrastructure, economy, and citizens.[118]

[109] Dunn Cavelty, 'Europe's Cyber-Power', 307.
[110] Dunn Cavelty, 'Cybersecurity between Hypersecuritization and Technological Routine', 306.
[111] Claessen, 'Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance', 153.
[112] Renda, 'The Development of EU Cybersecurity Policy', 469.
[113] Mărcuț, 'Evaluating the EU's Role as a Global Actor in the Digital Space', 81–82.
[114] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy'.
[115] Renda, 'The Development of EU Cybersecurity Policy', 469–70.
[116] Fritzsche and Spoiala, 'The EU-AU Digital Partnership', 24.
[117] Erforth and Martin-Shields, 'Where Privacy Meets Politics: EU-Kenya Cooperation in Data Protection', 142.
[118] Monsees and Lambach, 'Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity', 381–88.

In this regard, the EU is attested an 'ontological insecurity,'[119] which sheds light on how the EU seeks to maintain a 'sense of self' in dealing with issues such as security, migration, trade, and global competition with China. In doing so, the EU finds itself in an "'eternal' struggle' as a global actor between its identity as a normative power and its realist interests."[120] This sense of self is rooted in historical imaginaries of colonial power. The lens of 'ontological (in)security' integrates the EU's normative approach and its desired strategic power for analysis of how the EU is pursuing European identity in a changing global landscape. This perspective goes beyond a simplistic dichotomy, that categorises normative values as 'good' and strategic or geopolitical interests as 'bad.'[121]

The EU advocates its soft power to become a normative actor and global standard setter, and is committed to a multilateral, multistakeholder governance approach in its external policy.[122] Its strategy and ambition is to externalise its European norms and values to strengthen its global position. Successful externalisation is measured by non-EU actors actively adopting or adhering to European regulation in line with EU policy and legislation. However, this is often limited to the phase of externalisation and legislation is not actually being adopted.[123]

Another approach to strengthening the global position is building 'strategic partnerships' with other states. Thereby, the EU focuses on collaborating especially with countries that are considered like-minded and share the same norms and interests.[124] However, developing partnerships with Global South countries is challenging as the EU acknowledges its limited influence and trust compared to China.[125] Despite investing in capacity building and diplomatic efforts, the EU has not been successful in gaining recognition as a reliable, long-term partner by African and Latin American countries, indicating limited success of its strategy.[126] Weaknesses in policy coherence, impact monitoring, and

[119] Orbie, 'The Graduation of EU Development Studies', 602.
[120] De Roeck, Delputte, and Orbie, 'Framing the Climate-Development Nexus in the European Union', 6.
[121] Orbie, 'The Graduation of EU Development Studies', 599–602.
[122] Christou and Simpson, 'The European Union, Multilateralism and the Global Governance of the Internet', 243; Dunn Cavelty, 'Europe's Cyber-Power', 313; Renard, 'EU Cyber Partnerships', 326.
[123] Erforth and Martin-Shields, 'Where Privacy Meets Politics: EU-Kenya Cooperation in Data Protection', 142–46.
[124] Renard, 'EU Cyber Partnerships', 322–25.
[125] Teevan, 'Building Strategic European Digital Cooperation with Africa', 4.
[126] Izycki, Van Niekerk, and Ramluckan, 'Cyber Diplomacy', 417–23.

establishing a sincere relationship on equal footing with partners are apparent in the EU's action.

Next to global influence, one of the primary goals of these efforts is to achieve digital sovereignty and strategic autonomy.[127] Being digitally sovereign or autonomous means that there is no need to rely on other countries or actors for one's own security and operability. Digital sovereignty is not necessarily indicated by military capabilities, but also by economic power as well as IT and infrastructure security. The EU assumes that being independent enables it to assume a global leadership position and ensure its own security. This is why privacy, data protection, and fundamental rights – the core pillars of the EU's international agenda – are central in the European discourse and form the basis of Europe's vision of achieving digital sovereignty.[128]

In conclusion, the question of whether the EU can be considered a cyber power or a digital actor with global influence remains a topic of debate among scholars such as Renard[129] and Mărcuț. Some argue that while the EU is a player or power, it does not qualify as a fully-fledged international actor. The EU is a unique 'project' with a special status in an international arena that is built by and for nation-states. On the other hand, the EU may count as an actor, but without a great deal of de facto global power, at least not as much as it would like to have. In this regard, a distinction can be made. Mărcuț suggests that while the EU may be a regulatory actor, it does not hold significant authority as a technological actor.[130] Conversely, Dunn Cavelty notes that many critics fault the EU for not possessing sufficient cyber power. However, the author argues that assessing cyber power solely in militaristic, hard power terms is a too simplistic and narrow approach when applied to the EU.[131] Ultimately, the question remains open to interpretation.

These four chapters on international development, cyber governance, international cybersecurity, and the EU as a global actor constitute the theoretical basis for my analysis.

[127] Claessen, 'Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance', 153; Carver, 'More Bark than Bite?', 1.
[128] Monsees and Lambach, 'Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity', 378–79.
[129] Renard, 'EU Cyber Partnerships', 326.
[130] Mărcuț, 'Evaluating the EU's Role as a Global Actor in the Digital Space', 79–83.
[131] Dunn Cavelty, 'Europe's Cyber-Power', 310.

Before presenting my methodological approach, I examine the literature on cyber capacity building.

4. Literature Study: Cyber Capacity Building

In this chapter, I provide a comprehensive overview of the CCB literature by looking at different trends in defining CCB, examining its main characteristics, highlighting particular tensions, and exploring how CCB can be seen as a tool of foreign policy.

Cyber capacity building (CCB) is an instrument that emerged in the mid-2000s at the intersection of cybersecurity and international cooperation. It is occasionally called *cybersecurity* capacity building or capacity *development*.[132] Research in this area is interdisciplinary, drawing from various fields, such as political science, security studies, development studies, and science and technology studies. While there is some empirical research,[133] it is worth noting that much existing literature is based on "logical reasoning, limited case studies, anecdotal evidence, and expert opinion […]."[134] Case studies on regional cyber capacities include for example Japan[135] and Poland,[136] or look more broadly at Europe[137] and Africa.[138] Most CCB research includes policy implications or is produced by an international organisation or think tank, like NUPI, EUISS, and ITU. I have excluded most of this literature from the academic body, except for a few essential and frequently referenced publications. It is worth noting that many of the academic authors are or were nevertheless affiliated with such institutions, and for the sake of transparency I indicate their affiliation at the time of publication, if applicable.

4.1. Definitional Clusters

CCB definitions can be categorised in several clusters. The most frequently cited scholar is Patryk Pawlak (EUISS). According to Pawlak, CCB is "an umbrella concept for all

[132] Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 298–302.
[133] Dutton et al., 'Cybersecurity Capacity. Does It Matter?'; Calderaro and Craig, 'Transnational Governance of Cybersecurity'.
[134] Dutton et al., 'Cybersecurity Capacity. Does It Matter?', 302.
[135] Bartlett, 'Why Do States Engage in Cybersecurity Capacity-Building Assistance?'
[136] Siudak, 'Cybersecurity Discourses and Their Policy Implications'.
[137] Creese et al., 'The Solution Is in the Details'.
[138] Calandro and Berglund, 'Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case'.

types of activities (e.g. human resources development, institutional reform or organizational adaptations) that safeguard and promote the safe, secure and open use of cyberspace."[139] Amazouz (African Union)[140] and Muller (NUPI),[141] among others, have adapted this conceptualisation, which focuses on developmental endeavours for the overarching ambition of creating a desired version of cyberspace.

In the second cluster, Homburger emphasises the importance of the (cyber-)security aspect in development. She adjusts the definition to "support and assistance aiming at empowering individuals, communities and governments to reduce risks stemming from access and use of information and communication technologies."[142] This version aligns with the statement in the UN GGE report in 2015, that states should "provide assistance and training to developing countries to improve security in the use of ICTs […]."[143] This cluster aims to enhance the overall level of security and minimise negative effects of digitisation on society.

In the third cluster, Calderaro and Craig refer to CCB as "the diffusion of technical, governance and diplomatic skills among relevant stakeholders, including government, industry and civil society actors, to ensure the development of sustainable connectivity."[144] This definition focuses on sharing and developing the skills and capacities of people and institutions to foster digitisation.

Fourthly, Hohmann et.al. (GPPi) define CCB as a „set of initiatives that empowers individuals, communities, and governments to reap potential gains from investments in digital technologies, or what the World Bank calls 'digital dividends.'"[145] This definition is focusing on how cyber capacities can be used for economic profit, which assumes that the digitisation of the economy leads to economic growth. Therefore, cybercrime and security

[139] Pawlak, 'Riding the Digital Wave', 6.
[140] Amazouz, 'Cyber Capacity-Building and International Security', 202.
[141] Muller, 'Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities', 5.
[142] Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace', 227.
[143] United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," para 21(b).
[144] Calderaro and Craig, 'Transnational Governance of Cybersecurity', 920.
[145] Hohmann, Pirang, and Benner, 'Advancing Cybersecurity Capacity Building. Implementing a Principle-Based Approach.', 4.

breaches pose a significant threat to the integrity of systems and networks, and by extension, the economic sphere.[146]

Collett (GFCE/UK diplomat) adds that CCB can also be characterised to "'build functioning and accountable institutions to respond effectively to cybercrime and to strengthen a country's cyber resilience.'"[147] This definition is adopted by the EU Operational Guidelines on CCB 2018 and aligns with Barberos and Berglunds (DCAF) definition,[148] which also emphasises the institutional capacities of states and international cooperation to tackle challenges of digitisation.[149] This version combines elements of previously mentioned definitions by focusing on cybercrime as the risk and a country's resilience as the aim, achieved through institution building.

4.2. Main Characteristics

In summary, CCB broadly involves building and enhancing technical, organisational, and human skills and resources to increase resilience and adaptability to realities of cyberspace. CCB can include creating policies and strategies, handling security incidents, promoting societal and cultural norms, providing education, establishing appropriate laws and law enforcement, and implementing the highest technological standards.[150] These activities can be categorised into three main dimensions: building individual capabilities at the civil-society level, organising structures at the multistakeholder level, and developing institutional and policy frameworks at the state actor-level. The development community sees CCB as a way to bridge the digital divide, ensure human rights online, fight poverty, and achieve sustainable development.[151]

The cyber capacity of a country can be influenced by various variables, including its wealth, total population, and the extent and centralisation of Internet usage. Dutton et.al.

---

[146] Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace', 226–27.
[147] European Union, "Operational Guidance for the EUs International Cooperation on Cyber Capacity Building"; as cited in Collett, "Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures," 303.
[148] Barbero and Berglund, 'Cybersecurity Capacity Building and Donor Coordination in the Western Balkans', 4.
[149] Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 303.
[150] Dutton et al., 'Cybersecurity Capacity. Does It Matter?', 281–84.
[151] Pawlak and Barmpaliou, 'Politics of Cybersecurity Capacity Building', 124–27.

have found that while wealth enables a country to invest in technical and educational capacity building, the ability and trust of end-users to safely navigate the Internet is crucial in lower-income countries to benefit from Internet use. End-user security depends less on wealth and more on capacity building activities, which are influenced by political choices. The authors conclude that cybersecurity capacity building is essential to enhance end-users' experience. The perspective of the pro-CCB community is that wealthier countries and international organisations should support CCB in lower-income countries to strengthen the global Internet security overall.[152] However, the literature reveals many nuances and tensions between different conceptualisations and ideas, of which I will outline a few.

4.3. Tensions in the Literature

There are differing definitions of CCB, as mentioned above. A particular critique of these definitions relates to the general global dynamic. Collett argues that most definitions and frameworks imply that Global North countries one-directionally develop Global South countries, which is a flawed and inadequate assumption. Instead, Collett identifies four possible directional models for CCB. In addition to the North-South dimension, capacity building can also take place between countries of the Global South (North-South-South). Another model involves the idea that countries of the North can benefit from CCB in or from the South (triangular model). The most comprehensive model that Collett describes additionally includes CCB between Global North countries, allowing any country to be part of a capacity building partnership with any other country (multidirectional type). All stakeholders can function as both 'givers' and 'takers' in cyber capacity building.[153]

Collett, however, does not problematise development per se. Hurel (RUSI) highlights that most definitions are situated in the context of development[154] such as Collett 2021, Pawlak 2016, Calderaro and Craig 2020, and Hohmann et.al. 2017.[155] The terms 'diffusion,'

[152] Dutton et al., 'Cybersecurity Capacity. Does It Matter?', 291–303.
[153] Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 303–4.
[154] Hurel, 'Interrogating the Cybersecurity Development Agenda: A Critical Reflection', 70.
[155] Calderaro and Craig, 'Transnational Governance of Cybersecurity'; Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures'; Hohmann, Pirang, and Benner, 'Advancing Cybersecurity Capacity Building. Implementing a Principle-Based Approach.'; Pawlak, 'Capacity Building in Cyberspace as an Instrument of Foreign Policy'.

'development,' and 'assistance' are recognisable from a postcolonially-informed, critical perspective vis-à-vis development rhetoric as an indication of a North-South dimension. Authors like Hurel, who are particularly critical of the traditional donor-recipient framework due to its postcolonial dimension, therefore see the necessity of questioning the concept of CCB as it is.

The North-South divide, which is inherently present in traditional development dynamics, poses a particular challenge: the experiences of the Global North cannot simply be applied to the Global South. The process of digitisation in Western countries has unfolded over a long time, with an alternating mix of state-led and private involvement. However, in the Global South, digitisation has progressed rapidly, and is primarily driven by the private sector, outpacing government efforts. Schia (NUPI) points out that this rapid shift does not leave sufficient time for the country to adapt its society, economy and policies to the digital reality, which leads to vulnerabilities that are not seen in the North. Concerns even arise regarding the potential of a digital technology-driven "third wave of imperialism."[156] Schia recommends prioritising the need to build the 'analogue foundations' first, including policy and infrastructure development, and to advance "development assistance to projects and activities focusing on awareness, knowledge, information, education and employment."[157]

However, tensions do not only point to difficulties with the concept of development as such. Various issues also arise within CCB. One question is determining the most vulnerable party. According to Ashgari et.al. (2015), lower-income countries with insufficient secure ICT infrastructure and skills are considered particularly vulnerable. Conversely, higher income countries heavily rely on Internet infrastructure which potentially renders them more at risk.[158] Additionally, Collett criticises the focus on a country's economic status as the key factor in CCB partnerships, arguing that CCB tends to be too state-centred and overlooks non-state communities' interests and goals.[159]

[156] Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South', 824.
[157] Schia, 824.
[158] Calderaro and Craig, 'Transnational Governance of Cybersecurity', 923.
[159] Collett, 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', 304–5.

According to Calderaro and Craig's research, cyber capacities are not primarily developed in response to external threats, domestic politics, or norms. Their study emphasises the importance of science and technical knowledge. They argue that advanced countries should therefore collaborate with Global South countries to improve education and skills in this area. This view contradicts the prevailing military paradigm in international relations, which is based on the deterrence theory and focuses on militarising digital technology as 'cyber weapons,' and attacks as 'cyberwar.'[160] This connects to the criticism towards the securitisation of cyberspace.

It becomes clear that there are discrepancies in how cybersecurity should be understood. The main difference lies in focusing on human security as opposed to state security. Looking at cybersecurity from a human security perspective prioritises the protection of society to ensure that everyone can safely access digital services in their everyday lives, while upholding fundamental rights.[161] Schia, for example, argues that digital development without a security perspective is unsustainable and can even lead to increased cybercrime if digital tools are subject to poor governance and poverty on the ground.[162] On the other hand, Egloff and Shires connect cybersecurity to state security, for example military capabilities.[163] This perspective views cybersecurity as a matter of state sovereignty.[164]

Furthermore, there is a notable tension concerning the transnational and cooperative versus the national sovereignty approaches to cyberspace and governance. Technically, both the human and the state security approach require a transnational approach because technical Internet infrastructure as well as behavioural norms are not functional if they are only discussed on a national or regional level. However, it is widely acknowledged that there is no global consensus on practically anything. States aim for digital sovereignty, by seeking control over physical hardware and digital software to protect themselves from cyber threats that could potentially harm their national integrity. Calderaro and Craig argue that cybersecurity should be approached with a national strategy while participating in transnational cybersecurity governance.[165] Homburger, however, sees an inherent

[160] Calderaro and Craig, 'Transnational Governance of Cybersecurity', 922.
[161] Calderaro and Craig, 920.
[162] Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South', 823.
[163] Hurel, 'Interrogating the Cybersecurity Development Agenda: A Critical Reflection', 70.
[164] Calderaro and Craig, 'Transnational Governance of Cybersecurity', 920.
[165] Calderaro and Craig, 921.

power imbalance in the global system and concludes that the states with more resources and knowledge in using ICTs have a more powerful position to shape global interactions, including assistance and cooperation between donor and recipient states.[166]

4.4. A Tool for Foreign Policy?

How does CCB fit into global politics and international political agendas? Pawlak recognises that CCB can function as a tool for foreign affairs and acknowledges that donor nations and organisations may have interests beyond the socio-economic development of recipient countries.[167] But what specific concerns might these be in the broader context of geopolitical and state agendas?

First, there are defensive self-interests rooted in a state-centred understanding of the international system. States are interested in CCB due to the security risk associated with the Internet's interconnected and transnational nature. A significant gap exists in cybersecurity capacities among nations worldwide, leaving many particularly vulnerable to threats. These vulnerabilities can spill over into other states and actors.[168] Because countries are dependent on each other's technology, regulations, state behaviour and cooperation, cyber-attacks can be perceived as a shared threat, especially among allied states.[169] Strengthening ties within regional and international constellations of countries can be beneficial and cost-effective, enhancing trust and interdependency for all parties involved.[170]

Second, CCB can go beyond just the national security and self-defence. It can function as a powerful tool for donor states to convey their economic, strategic, and security interests, as well as norms and values to recipient states. This suggests that CCB is not merely a neutral and generous activity, but "[…] can serve as a tool to foster geopolitical interests in the field of cybersecurity."[171]

---

[166] Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace', 228.
[167] Pawlak, 'Capacity Building in Cyberspace as an Instrument of Foreign Policy'.
[168] Amazouz, 'Cyber Capacity-Building and International Security', 203; Dutton et al., 'Cybersecurity Capacity. Does It Matter?', 303.
[169] Hurel, 'Interrogating the Cybersecurity Development Agenda: A Critical Reflection', 77.
[170] Bartlett, 'Why Do States Engage in Cybersecurity Capacity-Building Assistance?', 481.
[171] Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace', 232.

This points to the role of CCB for broader cyberspace governance, for example as a component of cyber diplomacy. Homburger argues that a certain level of cyber capacity is necessary for implementing cyber norms and laws, making capacity building an instrument for broader objectives of creating a common international cyber system. [172] Conversely, Pawlak and Barmpaliou contend that CCB needs to be based on rules and principles to prevent potential misuse of cyber tool, given their inherent dual-use nature.[173] Izycki et.al. discuss shortcomings of capacity building, which can have negative effects on cyber diplomacy. Often, CCB efforts are not comprehensive and inclusive enough to fully meet the needs of recipient countries. The donor countries' engagement tends to privilege a few stakeholders, while neglecting local small and medium-sized enterprises in cybersecurity consulting. Despite the increased attention and projects aimed at building capacities and confidence in Africa and Latin America, many of these countries have still not been able to join the group of 'like-minded' countries that the EU considers most aligned with its vision, especially in serious discussions and cooperations on cybersecurity and defence.[174] This indicates a biased diplomatic cooperation that has the potential to frustrate partner countries.

Craig et. al. highlight that major powers appear to be more committed to the international, collaborative approach than smaller powers. More powerful states are more likely to advocate for norms and CCB to gain greater international influence over others and to assert their position in the international arena.[175] However, whether CCB is aimed at achieving security or if it is meant to be a tool for enabling broader political, social and economic transformations depends on how it is employed and interpreted.

5. Methodology

This section sheds light on my methodological considerations and procedure. My research is situated within the field of global studies, which prioritises critical thinking, interdisciplinarity, acknowledging subjectivity, and the need to historically contextualise phenomena. From an epistemological standpoint, I adopt a social constructivist perspective.

[172] Homburger, 232.
[173] Pawlak and Barmpaliou, 'Politics of Cybersecurity Capacity Building', 135.
[174] Izycki, Van Niekerk, and Ramluckan, 'Cyber Diplomacy', 423–24.
[175] Craig, Johnson, and Gallop, 'Building Cybersecurity Capacity', 379–91.

Social constructivism highlights that social phenomena and their meanings are not inherent, but are continuously created, modified and framed by social actors.[176] My methodological approach is interpretive, which allows me to understand subjective meanings and ambiguities. Interpretation has become a standard approach in policy analyses.[177]

For this approach it is essential to acknowledge my positionality as a researcher. My research, including the theoretical chapter, is shaped by my cultural, social, and academic background, which influences how I interpret the EU's global actions and their implications. As a scholar from Europe, with academic training in European and Global Studies, I bring a perspective that is both informed by and critical of Western-centric thinking. My aim is to deconstruct the EU's global strategies and policies through a lens that recognises historical and ongoing power imbalances. However, I am not in a position to actually highlight overlooked voices, promote equal representation, examine the practical impact of the EU's actions on the ground or be confident in my ability to fully challenge Eurocentrism and privilege.

5.1. Critical Frame Analysis

Frame Analysis has been used in a wide range of disciplines, including communication and media studies, political science, and policy studies. Frame Analysis helps to identify underlying meanings and narratives that are constructed strategically or implicitly, examining how an actor is "bending their meaning in certain directions."[178] Through framing, actors select aspects of reality such as different interpretations, ideas, or opinions and thus have a powerful impact on the outcome of decision-making processes. Framing has been described as "ways of world-making."[179] Frames are not neutral, but rather "organising principle that transforms fragmentary or incidental information into a structured and meaningful problem, in which a solution is implicitly or explicitly included."[180]

---

[176] Flick, Steinke, and von Kardorff, 'What Is Qualitative Research? An Introduction to the Field', 6–7. *See Berger and Luckmann 1966.*
[177] Van Hulst et al., 'Discourse, Framing and Narrative', 1.
[178] Lindekilde, 'Discourse and Frame Analysis: In-Depth Analysis of Qualitative Data in Social Movement Research', 200.
[179] Goodman, "Ways of worldmaking." Quoted from Van Hulst et al., 'Discourse, Framing and Narrative', 9.
[180] Verloo, "Mainstreaming Gender Equality," 20. Quoted from De Roeck, Delputte, and Orbie, 'Framing the Climate-Development Nexus in the European Union', 437–38.

I choose to conduct frame analysis to understand how the EU perceives itself as a global digital actor and how it frames – what meaning it gives – to the issue of cybersecurity and CCB. I aim to identify problems and solutions related to cybersecurity, explore different ways to perceive the international development of cybersecurity, and uncover underlying narratives, ideologies, and strategies.

Framing includes three steps: naming and describing the issue with the use of language, selecting aspects as relevant or irrelevant, and presenting a coherent narrative.[181] Political actors and policymakers, including the EU, actively engage with issues which they identify as 'concerning,' 'worrisome,' or 'urgent.' This process involves emphasising one issue over another and conveying it as important through vocabulary, thus requiring specific measures and attention.

To make frame analysis in policy studies more accessible, it can be divided into two parts: diagnosis – what is the problem presented to be, and prognosis – what are the possible solutions introduced. It is important for my research to additionally be critical, considering the potential power imbalances, biases, and structural inequalities among different stakeholders.[182]

In the selection of my frames, I rely on findings from the literature review to identify relevant frames. As I progress through the research process, I am open to adjust, include or disregard frames. Possible frames I include are economic, security, technological, legal/regulatory, international cooperation, social, political, cultural, ethical/human rights, geopolitical, developmental, and solidarity. Additionally, I consider the top-down and the bottom-up dimension to analyse whether the EU imposes problems and solutions onto the local situation, or whether the agency and context of local actors is engaged in the EU's activities.

The economic frame focuses on the economic and financial dimension of cybersecurity and includes aspects such as cost-benefit analysis, market growth, and financial incentives to improve cybersecurity. This frame assesses whether a lack of cybersecurity is

[181] Van Hulst and Yanow, 'From Policy "Frames" to "Framing"', 5.
[182] De Roeck, Delputte, and Orbie, 'Framing the Climate-Development Nexus in the European Union', 2.

perceived as a threat to growth, and if economic and financial development measures are considered a solution to cybersecurity shortages.

The security frame emphasises the broader EU and international security and considers cyber threats from state and non-state actors, defence measures and strategies, national interests and critical infrastructure as well as global peace and stability. Throughout the analysis, I noticed a military framing, that categorises cyberspace and cybersecurity within a military rhetoric and agenda. However, the military rhetoric ties in with the security framing, which is why I label military a subcategory of security. There is a distinction between realist security framing, which focuses on the state-level, and the human security framing, which concerns the well-being of individuals and communities.

The technological frame promotes the advancements and utilisation of software tools and technological innovations to combat cyber threats and enhance infrastructure and expertise. This perspective suggests that technology is seen as the primary driver of societal change, potentially indicating the concept of technological determinism. It can be interpreted as the belief that cybersecurity issues can be addressed through technological development, or that the implementation of secure technologies contributes to broader social, economic, and political development, which means that technological solutions are used to tackle challenges beyond technological issues.

The legal/regulatory frame refers to legal and regulatory measures like developing or improving policies, laws, directives, and frameworks that are used to govern, enforce, and enhance cybersecurity. This relates to the broader implication of a governance-centric and institutional approach to managing cybersecurity challenges. This frame takes a rather state-centred lens, focusing on the role of governments and institutional authority, with the risk of promoting a homogenised approach to addressing a wide range of issues across different actors through standardisation and regulation.

The international cooperation frame focuses on global collaboration in bilateral or international fora, international policies, standards, and agreements as well as the EU's role in global cybersecurity initiatives. This frame emphasises the idea of cybersecurity as a matter of collective security and shared responsibility and advances the globalisation of cybersecurity efforts. It also involves the questions of leadership roles and reaching global

consensus across various states, connecting to broader international considerations in different policy domains.

The social frame examines the impact of cybersecurity on society and individuals, including public awareness, individual responsibility, and education and training to improve people's skills and address the societal impact of cyber threats and security. This frame connects to the human security interpretation of cybersecurity and emphasises the 'people' or 'human-centric' approach advocated by the EU. It also underscores the role of cybersecurity for societal well-being, suggesting that cybersecurity development is a matter of social equality and justice, for example for marginalised communities. However, there is a risk of employing a top-down neoliberal understanding of empowerment and justice, which disregards redistribution and local agency.

The political frame is concerned with political implications related to cybersecurity, such as political agendas and motivations, government actions, political parties, elections or legislative debates and decisions. This reflects the perception that cybersecurity is a critical component of political strategy and governance. If this perspective is employed from the top-down, it concentrates on national governments and high-level decision-making. From the bottom-up, it focuses on political engagement of local communities, civil society organisations, and citizens.

The cultural frame emphasises cultural norms, values, behaviour, and cultural attitudes that influence the use of technology and cybersecurity. This analysis can help in developing culturally sensitive and adaptive solutions. However, there is a risk that the cultural frame may be used to diagnose problems based on a lack of cultural understanding or the absence of certain norms and values.

The ethical/human rights frame considers individual rights and liberties, and the ethical and moral implications of cybersecurity practices and policies. This includes the ethical use of technologies, moral responsibilities of actors, and privacy as well as surveillance concerns. Ethics and human rights are summarised as one frame because they often overlap. This frame is rather top-down, with the tendency to view human rights as having universal validity, and the EU being the one that determines ethical considerations. It also

refers to a normative claim about what constitutes ‘good’ behaviour and the ideals of a better world.

The geopolitical frame examines international relations, strategic power dynamics, interests, and the influence of cybersecurity on global politics. This includes cyber warfare and espionage, international diplomacy, as well as strategic power relations and interests. In comparison, the security frame focuses on protecting one’s own security and integrity against crime and threats, including the operationality of infrastructure and systems, whereas geopolitics is more about the distribution of international interests and power among states.

The developmental frame focuses on the role of cybersecurity in international development. Cybersecurity can be seen as a fundamental element for successful international development with the potential to contribute to the SDGs by building (digital) infrastructure, enhancing capacities, and narrowing the digital divide. However, cybersecurity could also be a necessary consequence of digitisation to ensure the integrity and functionality of new digital systems. In my analysis, the developmental frame has an inherently global dimension, expectedly along the North-South axis.

The solidarity frame emphasises collective efforts and shared responsibilities in addressing cybersecurity challenges among nations, governments and individuals. It involves collaboration, mutual support, assistance, and community efforts based on goodwill and global solidarity. This can stem from the realisation that everything is globally connected. Based on this belief, harm for others can have negative implications for oneself, reflecting how self-interest is intertwined with altruism. It can also imply a sense of duty to take on global responsibility and share resources.

For a better overview, I have summarised the frames in the following table and added critical considerations, which connect to the theoretical framework:

Frame	**Diagnosis (Problem presented)**	**Prognosis (Solutions introduced)**	**Critical considerations**

Economic	Risks to economic growth and financial stability	Financial incentives, market growth strategies, economic development measures	Power imbalances, profit prioritisation, critique of neoliberalism
Security	Threats to national/international security and critical infrastructure	Defence measures, security strategies, military agenda	Militarisation/Securitisation of cyberspace, state vs. human security, civil liberties impact
Technological	Technological inadequacies as the root of cybersecurity issues	Technological development, innovation, expertise enhancement	Technological determinism and solutionism
Legal/regulatory	Inadequate legal frameworks leading to cybersecurity vulnerabilities	Policies, laws, directives, governance frameworks	Top-down regulation, centralisation of power, local context disregard, homogenisation
International cooperation	Cybersecurity as a global issue requiring global action	International agreements, collaborations, EU leadership in cybersecurity	Power dynamics, imposition of European standards and norms, ability to reach consensus
Social	Threats affecting societal well-being, lack of public awareness	Public education, awareness campaigns, skills development	Interpretation of empowerment, engagement with marginalised communities
Political	Cybersecurity as a necessary component of political strategy and governance	Political agendas, legislative debates, government actions	Politicisation of cybersecurity, focus on high-level decision-making and marginalisation of local communities
Cultural	Cultural differences influencing cybersecurity perceptions and technology use	Culturally sensitive and adaptive solutions	Cultural imposition risks, stereotyping, marginalisation of non-Western perspectives

Ethical/human rights	Cybersecurity practices infringing on individual rights and ethical standards	Ethical standards promotion, human rights protection, privacy considerations	Paternalistic approaches, universalising Western ethics, overlooking the local context
Geopolitical	Competing strategic interests and power dynamics, espionage, warfare	Strategic role of cybersecurity in diplomacy and international relations	International power imbalances, impact on global cooperation, increased tensions
Developmental	Cybersecurity as prerequisite for sustainable development and bridging the digital divide	Integration into development programs, capacity-building, support for SDGs	Reinforcement of inequalities, neglect of local priorities, instrumentalisation for self-interests
Solidarity	Collective efforts and shared responsibility needed for cybersecurity challenges	Global cooperation, mutual support, community-driven approaches, goodwill	Balancing self-interest with altruism, Europe's global responsibility
Top-Down	EU imposes cybersecurity solutions onto local contexts, lack of contextual understanding	Improved alignment and contextual adaptation of policies, enhanced collaboration, power redistribution	Marginalisation of local voices, one-size-fits-all approach
Bottom-Up	Local actors identify cybersecurity issues and develop context-specific solutions	Grassroots initiatives, local capacity-building, unconditional support	Local agency, context-sensitive efforts, effectiveness of local involvement

1 Analytical Frames

5.2. Data Selection

The documents are selected in a time frame from 2013, which is when the first Cybersecurity Strategy was released, to 2024. I examine international cyber capacity building in third countries, which means outside of the EU. Since the EU includes international cybersecurity in its internal policies and strategies, I am looking into a selection of these as well. I located the documents through research on EU websites and cross-references within publications. The documents can include all sorts of publications from EU

institutions, agencies, and institutes. However, most of them are published by the European Commission (referred to as the Commission) and the Council of the EU (referred to as the Council).

I selected the documents according to their relevance to my research focus. This depended on whether cybersecurity was considered in an international context, or if 'digital development' or 'cyber capacity building' came up in the keyword search. Additionally, I consider a range of broader strategies that inform and include cyber policy, even if they do not directly focus on international cybersecurity or CCB as their main topics. I also added selected cyber diplomacy documents, as CCB is not just related to cybersecurity, but a part of EU cyber diplomacy. In the end, I analysed 25 documents covering CCB and aspects of digital development (referred to as 'Digital4Development'), cybersecurity, and cyber diplomacy. The documents were coded using Excel. This allowed more flexibility in defining and adapting (multiple) frames. I categorised the documents into four sections. However, in the analysis, I integrated the four chapters into two to get a cohesive picture and avoid too much repetition.

For the section on Cyber Capacity Building, I have analysed the following documents.

No.	**Title**	**Institution**	**Date**
1	Cyber capacity building: towards a strategic European approach	Council of the EU	30 June 2016
2	Mainstreaming digital solutions and technologies in EU development policy – Council conclusions	Council of the EU	28 November 2016
3	Commission staff working document. Digital4Development: mainstreaming digital	European Commission	02 May 2017
4	Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final text	Council of the EU	09 October 2017

5	Digital4Development - Council conclusions	Council of the EU	20 November 2017
6	EU External Cyber Capacity Building Guidelines - Council conclusions	Council of the EU	26 June 2018
7	Operational Guidance for the EU's international cooperation of CCB	EUISS, European Commission	2018
8	International Cyber Capacity Building: Global trends and scenarios. Annex 3. Notes on CCB Funders	European Commission	September 2021
9	Mapping of EU-funded External Cyber Capacity Building Actions 2022	European Commission, EU CyberNet	2022

2 Cyber Capacity Building Documents

I have analysed four documents for cyber diplomacy, among them one that I have also included in the category CCB.

No.	**Title**	**Institution**	**Date**
4	Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - approval of the final text.	Council of the EU	09 October 2017
10	Council Conclusions on Cyber Diplomacy	Council of the EU	11 February 2015
11	Understanding the EU's approach to cyber diplomacy and cyber defence	European Parliamentary Research Service	May 2020
12	Council Conclusions on EU Digital Diplomacy	Council of the EU	26 June 2023

3 Cyber Diplomacy Documents

For the section on strategic global frameworks, I selected six documents. These documents are referenced multiple times in CCB and cybersecurity-related documents as guiding documents.

No.	**Title**	**Institution**	**Date**
13	The European Agenda on Security	European Commission	28 April 2015
14	Global strategy for the European Union's Foreign and Security Policy	European Commission	June 2016
15	The New European Consensus on Development: 'Our World, Our Dignity, Our Future'	European Parliament, Council of the EU, European Commission	29 February 2020
16	Shaping Europe's digital future	European Commission	21 March 2022
17	A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security	Council of the EU	21 March 2022
18	Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - Progress Report	Council of the EU	20 November 2023

4 Strategic Frameworks

I have analysed the following documents on cybersecurity.

No.	**Title**	**Institution**	**Date**

19	Cybersecurity Strategy of the EU	European Commission	07 February 2013
20	EU Cybersecurity Initiatives working towards a more secure online environment – Factsheet	European Commission	January 2017
21	Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	European Commission	13 September 2017
22	The EU's Cybersecurity Strategy for the Digital Decade	European Commission	16 December 2017
23	Report on implementation of EU's Cybersecurity Strategy for the Digital Decade	European Commission	23 June 2021
24	Council Conclusions on the EU Policy on Cyber Defence	Council of the EU	22 May 2023
25	Council Conclusions on the Future of Cybersecurity: implement and protect together	Council of the EU	21 May 2024

5 Cybersecurity Documents

In the following chapter, I present the results of the analysis in detail. In the first section, I analyse how the EU sees and represents itself as a global actor more broadly. In the second section, I examine how the EU frames cybersecurity and CCB more closely.

6. Analysis

6.1. Positioning the EU as a Global Actor

"Thinking global, acting European"[183]

[183] European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade', 4.

In its approach to cyberspace, the EU emphasises security, prosperity, and the promotion of democracy and a rules-based international order. However, the EU feels increasingly "under threat" in terms of its general security and integrity.[184] There are significant geo-political concerns regarding conflicts, not only in the 'traditional' sense, but also in cyberspace, for example concerning the authoritarian use of cyber tools. The EU regards cyberspace as a domain of operations like land, air and sea.[185] It is considered a strategic and global space, with international implications for everything.[186] This comprehensive strategy reflects the EU's ambition to frame itself as a meaningful global actor and preserve European norms and values on the world stage.

The EU emphasises the interconnectedness of internal and external security,[187] asserting that cybersecurity is perceived as a shared threat and the security of its citizens and territory therefore depends on achieving peace and stability in the international system. This approach is particularly relevant in the neighbourhood regions, where enhancing resilience, capacities, and security is considered crucial for both regional and EU security.[188] With a large of the economy and everyday life relying on digital technologies,[189] it is considered a serious concern, indicating the urgency of taking action to confront the issue. However, cybersecurity "cannot be tackled in a vacuum."[190] As a result, cybercrime is one of the top priority areas for the EU's domestic and international agenda on security.

The EU is committed to safeguarding its citizens against cybercrime, focusing on data protection, privacy, and compliance with fundamental rights online[191] (ethical/human rights frame). A coordinated response to emerging threats is a central goal of the EU's security strategy.[192] The EU believes that collective and coordinated measures can have a tangible impact in addressing cyber threats (international cooperation frame), which are

[184] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 7.
[185] European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 17.
[186] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 11.
[187] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 7.
[188] European Union, 26.
[189] European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 2; European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade', 1; General Secretariat of the Council, 'Council Conclusions on the EU Policy on Cyber Defence', 2.
[190] General Secretariat of the Council, 'Council Conclusions on the Future of Cybersecurity: Implement and Protect Together', 19.
[191] European Commission, 'The European Agenda on Security', 3–4.
[192] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 9.

seen as "borderless, flexible and innovative."[193] These threats have the potential to violate fundamental rights and can even escalate to the level of "cyber-terrorism," (military/security frame) leading to severe economic and financial consequences.[194] Recognised as a core pillar in defending against cybercrime, cybersecurity is considered essential for maintaining an open and free cyberspace while protecting privacy and critical infrastructure against threats.[195]

Therefore, the EU advocates a "rules-based global order" rooted in multilateralism and anchored by the UN (international cooperation frame). On international stage, "national ownership and shared responsibility"[196] are important to be maintained. Guided by "principled pragmatism," the EU combines a "realist assessment of the current strategic environments" and the "idealistic aspiration to advance a better world."[197]

The concept of cyber diplomacy is an essential pillar of this approach. For the EU, cyber diplomacy is part of the broader Common Foreign and Security Policy (CFSP)[198] and "coexists with its sister strand of cyber defence, cyber deterrence and cybersecurity."[199] Diplomacy is based on principles of transparency, responsibility, and trust, for example through CBMs and CCB with international partners. Cyber diplomacy efforts target the promotion of responsible behaviour and the protection of human rights in security and defence.[200] The establishment and implementation of cyber norms are regularly recommended, although it is always noted that they are voluntary and non-binding.[201]

In context of diplomacy, the existing legal frameworks serve as a foundation for all international state behaviour. These frameworks include the UN Charter, the Universal Declaration of Human Rights, the EU Charter of Fundamental Rights, the Tallinn Manual,

[193] European Commission, 'The European Agenda on Security', 19.
[194] European Commission, 13.
[195] European Commission, 19.
[196] European Parliament, European Commission, and Council of the European Union, 'The New European Consensus on Development: "Our World, Our Dignity, Our Future"', 1.
[197] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 8.
[198] General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 5.
[199] Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 1.
[200] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 25–26; European Commission, 'Shaping Europe's Digital Future', 14.
[201] General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 6–8; Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 2–3.

and the Budapest Convention on Cybercrime, among others, and regulate and condemn malicious cyber behaviour.[202] Cyber diplomacy is framed as a matter of adhering to existing international legal instruments (legal/regulatory) and cooperative forums (international cooperation), as well as appealing to ethical and human rights-compliant behaviour (ethical/human rights frame).

Regarding development, the *European Consensus on Development* asserts that the EU bases all its development policies on achieving the SDGs and the 2030 Agenda for Sustainable Development. The aim of the Agenda 2030 is to eliminate poverty and achieve sustainable development globally by balancing economic, social and environmental interests, and promoting inclusivity and global peace.[203] The EU aspires to act as an "enabler" for development goals and a driving force for the implementation of the 2030 Agenda.[204] The 2030 Agenda is also seen as being in Europe's own interests for a more sustainable, inclusive, secure and prosperous future.[205] It is considered crucial to combine developmental efforts such as infrastructure investments "with the strategic promotion of *our* [emphasis added] technological solutions and standards."[206] This should be done while engaging in dialogues and addressing risks of digitisation to mitigate the digital transformation. Mobilising partners is essential to establish a common vision for development based on the EU's values and principles. This statement points to a top-down perspective on the developmental framing of technology, while also referring to international cooperation and standardisation.

The EU considers its principles and values as universal and indivisible, such as human rights, fundamental freedoms, gender and social equality, and solidarity (ethical/human rights frame). The EU states that all actions are guided by a rights-based approach to development cooperation, with a focus on maintaining "development effectiveness and ownership of development priorities in development countries, inclusive development

[202] General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 4.
[203] European Parliament, European Commission, and Council of the European Union, 'The New European Consensus on Development: "Our World, Our Dignity, Our Future"', 1.
[204] European Parliament, European Commission, and Council of the European Union, 16.
[205] European Parliament, European Commission, and Council of the European Union, 2.
[206] General Secretariat of the Council, 'Council Conclusions on EU Digital Diplomacy - Council Conclusions', 8.

partnerships, transparency and mutual accountability."[207] The EU seeks to diversify its development approaches and tailor its development partnerships to the specific needs and capacities of each country.[208] Therefore, in its recent development strategies, the EU strives for coherence, consistency, credibility and joined-up action,[209] with the goal of providing "added value, influence and a positive impact on the world."[210]

The EU's Digital4Development approach focuses on harnessing the potential of digital technologies. The aim is to enhance connectivity, increase accessibility, and make digital technologies more affordable for a larger portion of the population in developing countries to unlock the full potential of digital technologies for sustainable development.[211] Capacity building, especially in Africa, is seen to promote and respect the SDGs, with technological development considered a means of achieving broader development goals.

The EU emphasises that "the digital transformation can only work if it works for all and not for only a few. It will be a truly European project – a digital society based on European values and European rules – that can truly inspire the rest of the world."[212] The EU aims to mainstream "digital solutions" into development efforts, foster a thriving digital economy, and empower people, particularly women and other marginalised groups, to achieve better social inclusion, democracy, and participation in the digital space[213] (social, developmental frame). However, the EU acknowledges that technologies are not a universal problem-solver and should be put to use as a tool for "public goods."[214] This statement diverges somewhat from the perspective of technological determinism, asserting that the mere existence of technology will not solve all problems. However, if used effectively, it is seen as bringing about positive change and immense benefits.

The EU presents itself as a global player, that "inspires" others around the world to tackle policy challenges. It believes it possesses the regulatory power, technological capabilities,

[207] European Parliament, European Commission, and Council of the European Union, 'The New European Consensus on Development: "Our World, Our Dignity, Our Future"', 3.
[208] European Parliament, European Commission, and Council of the European Union, 16–19.
[209] European Parliament, European Commission, and Council of the European Union, 2–3.
[210] European Parliament, European Commission, and Council of the European Union, 3.
[211] European Parliament, European Commission, and Council of the European Union, 13.
[212] European Commission, 'Shaping Europe's Digital Future', 15.
[213] European Parliament, European Commission, and Council of the European Union, 'The New European Consensus on Development: "Our World, Our Dignity, Our Future"', 13.
[214] European Commission, 'Shaping Europe's Digital Future', 15.

and diplomatic strengths required to "advance the European approach and shape global interactions."[215] This is encapsulated in the belief of the 'Brussels Effect,' which drives the EU to "actively promote its model of a safe and open global Internet."[216] The EU stresses the importance of being guided by a "strong sense of responsibility" while also underlining the necessity of promoting human rights and addressing root causes of conflict and poverty.[217] Its core values, both online and offline, encompass freedom of expression, data protection and privacy, access for all, and a democratic and multistakeholder governance based on shared international responsibility[218] (top-down international cooperation, ethical/human rights frame).

Next to multilateral forums, the EU aims to engage in bilateral political dialogue and establish "strategic partnerships"[219] with countries such as the US, China, Japan, India, South Korea, Brazil.[220] These countries are considered "like-minded partners who share our values and high standards."[221] Partnerships should be grounded on mutual trust and confidence, respect for human rights, and addressing security concerns,[222] with a focus on "the common cyber good."[223] The EU intends to employ strategies like "signalling," "strategic communication," and "influencing,"[224] but is also open to sanctions or self-defence in response to an armed attack.[225]

Furthermore, cooperation with international partners is also seen from a geopolitical perspective[226] and is considered crucial for maintaining and strengthening "our geopolitical posture."[227] The EU seeks to build and maintain alliances with third parties to prevent

[215] European Commission, 13.
[216] European Commission, 13.
[217] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 42–43.
[218] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 3–4; European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 18.
[219] Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 8.
[220] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 12.
[221] European Commission, 'Shaping Europe's Digital Future', 14.
[222] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 12.
[223] Lațici, 'Doc 11: Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 1.
[224] General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 7.
[225] General Secretariat of the Council, 9–10.
[226] European Commission, 'Shaping Europe's Digital Future', 13.
[227] General Secretariat of the Council, 'A Strategic Compass for Security and Defence - For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security', 47.

cyberattacks, advance deterrence, and contribute to a more stable and secure cyberspace[228] (geopolitical/realist security frame). Additionally, the EU aims to prevent states from using international platforms or standardisation processes to promote their own political and ideological agendas, as these "often do[es] not correspond with the values of the EU."[229]

The EU positions itself as a leader[230] or in a "key role,"[231] for example, by using the formulation "EU-led dialogues."[232] These political dialogues on cyber and security aim to spread international awareness and communicate the EU's strategic orientation.[233] The EU wants to promote and strengthen its "political, economic and strategic interests,"[234] and have its "core EU values of democracy, human rights and the rule of law"[235] reflected. Additionally, it seeks to "advance European growth, prosperity and competitiveness,"[236] with the objective to improve security, "take advantage of the booming global cybersecurity market,"[237] and secure "sustainable access to the global commons."[238]. These efforts are seen as a means to earn respect for the EU's geopolitical, economic and regulatory power.

> *A Global Digital Cooperation Strategy will put forward a European approach to the digital transformation that builds on our long and successful history of technology, innovation and ingenuity, vested in European values, including openness, and will project them onto the international stage and engage with our partners.*[239]

This indicates an international cooperation framing, which is, however, based on geopolitical and security interests. The EU is acknowledging the risk that other powers could

[228] European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 18.
[229] European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade', 20.
[230] General Secretariat of the Council, 'Council Conclusions on EU Digital Diplomacy - Council Conclusions', 2.
[231] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 7.
[232] General Secretariat of the Council, 6–8.
[233] General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 6.
[234] General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 2; General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 11.
[235] General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 3; General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 5.
[236] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 4.
[237] European Commission, 'EU Cybersecurity Initiatives Working towards a More Secure Online Environment - Factsheet', 2.
[238] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 42–43.
[239] European Commission, 'Shaping Europe's Digital Future', 14.

take advantage of an empty sphere of influence if the EU does not actively promote for its values and interests,[240] especially in the EU's neighbourhood. It recognises that cyberspace has become a battleground for strategic competition, as society relies more on digital technologies.[241] To address these challenges, the EU aims to strengthen its own resilience and leadership position, as well as that of its partners, against hybrid and cyber threats in Africa, the neighbourhood, Western Balkans, and the Latin America and Caribbean region. Interestingly, regarding the Indo-Pacific region, cyber threats are not mentioned.[242]

In the *Strategic Compass for Security and Defence*, the EU observes a resurgence of power politics and emphasises the "indivisible" nature of its security. The EU also expresses concerns about the impact of cyber tools, battle of narratives, sovereigntist power politics, and the use of force and coercion in an increasingly contested cyberspace.[243] "Cyberspace is increasingly exploited for political and ideological purposes, and increased polarization at the international level is hindering effective multilateralism."[244] The EU is concerned about the "race for cyber superiority"[245] and the "push for 'cyber sovereignty,'" which could lead to fragmentation and the disruption of cooperative efforts.[246] This "threatens" the core values of the EU and the idea of a global, open cyberspace. The EU also sees this as a potential danger to the EU's unity or position in the world, again hinting at a geopolitical concern.[247] To address these challenges, the EU aims to be a "cyber player, protecting our critical assets and values in the digital world, notably by promoting a free and secure global Internet,"[248] thus reacting with normative claims. This ambition is part of a broader geopolitical strategy, where the EU intends to

[240] General Secretariat of the Council, 'A Strategic Compass for Security and Defence - For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security', 8.
[241] General Secretariat of the Council, 12.
[242] General Secretariat of the Council, 42–43.
[243] General Secretariat of the Council, 5–7.
[244] European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade', 2.
[245] Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 1.
[246] Lațici, 2.
[247] General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 8.
[248] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 42.

"mobilise our unparalleled networks, our economic weight and all the tools at our disposal in a coherent way" to achieve its priorities.[249]

The EU is specifically drawing attention to Russia's military aggression against Ukraine, along with the resulting geopolitical concerns, strategic competition, security threats, and military instability. These issues pose a substantial risk and concern for the EU, its neighbourhood, and the international system. As examples, the EU points out the use of hybrid threats and the "weaponisation" of soft power, the use of data and technology standards as instruments of political competition,[250] the spread of disinformation, and interference in the digital space of other countries.[251] In addition to Russia, the EU notes the competition with China, which utilises cyber tools and hybrid instruments to impact regional and global security. Consequently, the EU underscores the importance of safeguarding what it considers as "our" values and interests, as well as the rules-based international order.[252]

Military framing is utilised to strengthen the gravity and seriousness of the situation. Examples are "the cyber realm has become something of a battlefield,"[253] a "domain of warfare,"[254] and "cyber-terrorism."[255] The EU highlights that a robust and cooperative defence industry is a vital prerequisite for the EU's autonomy of decision and action.[256] The idea of becoming "strategically autonomous" and "technologically sovereign" through a comprehensive defence and diplomacy strategy is identified as a solution to the security challenges of cyberspace.[257] However, the EU acknowledges that, at this point, only the US and China may effectively achieve cyber sovereignty.[258]

---

[249] European Union, 10.
[250] General Secretariat of the Council, 'A Strategic Compass for Security and Defence - For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security', 2.
[251] General Secretariat of the Council, 'Council Conclusions on EU Digital Diplomacy - Council Conclusions', 9.
[252] General Secretariat of the Council, 'A Strategic Compass for Security and Defence - For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security', 8.
[253] Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 4.
[254] European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 2.
[255] European Commission, 'The European Agenda on Security', 13.
[256] European Union, 'A Global Strategy for the European Union's Foreign And Security Policy', 10–11.
[257] Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 1; General Secretariat of the Council, 'Council Conclusions on EU Digital Diplomacy - Council Conclusions', 2.
[258] Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 4.

The EU is concerned about the concentration of critical digital and internet governance services in the hands of "a few private companies," as it leaves "the European economy and society vulnerable to disruptive geopolitical or technical events."[259] The EU sees 5G as a geopolitical concern for technological sovereignty and autonomy, linking geopolitical and technical considerations.[260] In *Shaping Europe's digital future*, the EU reiterates the need to be a "strong, independent and purposeful digital player,"[261] as a basis for social, political and economic development,[262] indicating an economically framed concern.

> *European technological sovereignty starts from ensuring the integrity and resilience of our data infrastructure, networks and communications. It requires creating the right conditions for Europe to develop and deploy its own key capacities, thereby reducing our dependency on other parts of the globe for the most crucial technologies. Europe's ability to define its own rules and values in the digital age will be reinforced by such capacities. European technological sovereignty is not defined against anyone else, but by focusing on the needs of Europeans and of the European social model. The EU will remain open to anyone willing to play by European rules and meet European standards, regardless of where they are based.*[263]

In summary, the most evoked frames were international cooperation, ethical/human rights, and legal/regulatory. Additionally, security, including military, and geopolitical framings were also employed. Other frames were used rarely or not at all in relation to my research focus. From this result I conclude that the EU sees itself as a global player, operating through multilateralism and international partnerships, and with strategic and geopolitical ambitions as a core. As cybersecurity and digital transformation are diagnosed as global issues, any response must take place at the global level as well. The SDGs, particularly focusing on poverty reduction and sustainable growth, are the overarching framework for achieving a minimum level of global cybersecurity with the aim to stabilise the international system. It is crucial for the EU to take a leading role in addressing these issues and tackling insecurities and tensions with its own values and norms. Therefore, the issue is portrayed by mainly focusing on security and geopolitical terms, with

[259] European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade', 2.
[260] General Secretariat of the Council, 'Council Conclusions on the Future of Cybersecurity: Implement and Protect Together', 21.
[261] European Commission, 'Shaping Europe's Digital Future', 3.
[262] European Commission, 'Report on Implementation of the EU's Cybersecurity Strategy for the Digital Decade', 1.
[263] European Commission, 'Shaping Europe's Digital Future', 2.

the EU emphasising its international development efforts and its ideas of ethical, human rights-based, and multilateral cooperation as a response.

6.2. Decoding the EU's Cyber Capacity Building Agenda

The global and borderless nature of the internet offers both opportunities and challenges. While it serves as a tool for progress, disparities in access to a secure and open internet remain a concern. The internet is recognised for its positive impact on people around the world. Therefore, Europe should assist third countries in improving connectivity and accessibility through technological or capacity development while ensuring security and integrity in cyberspace.[264]

Cybersecurity capacity building is considered a key aspect in global cybersecurity. The EU acknowledges the connection between cyber resilience and sustainable development, with objectives focusing on technology, politics, regulations, and international cooperation in cybersecurity.[265] The EU is convinced that all countries should be "able to reap the social, economic benefits of the Internet and the use of technologies."[266] CCB is positioned within the security-development nexus[267] and is considered a prerequisite to advancing cybersecurity for digital infrastructure and ensuring a secure, responsible digital transformation for everyone. This, in turn, contributes positively to the EU's collective cybersecurity.[268] In this framing, cybersecurity is seen as a contribution to broader development goals. Concurrently, development in the form of CCB is regarded as the solution to tackle cybersecurity issues, while also tying it to self-interests.

Cyber capacity building is also seen as a strategic part of cyber diplomacy.[269] Important issues for the EU such as human rights, security, growth, and development should be approached as part of a comprehensive global strategy in cyberspace.[270] Cyberspace is

[264] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 16.
[265] European Commission, 'EU Cybersecurity Initiatives Working towards a More Secure Online Environment - Factsheet', 7.
[266] European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade', 22.
[267] General Secretariat of the Council, 'Council Conclusions on the Future of Cybersecurity: Implement and Protect Together', 19.
[268] General Secretariat of the Council, 20.
[269] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 9; Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 2.
[270] Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 6.

considered to be "important for continued global development and prosperity."[271] As digitisation is considered of global interest,[272] cybersecurity and a free, open cyberspace become a global challenge.[273]

The EU aims to provide and support inclusive and reliable access for third countries in line with its vision of fostering "international solidarity." [274] The metaphor "A chain is only as strong as its weakest link"[275] is used by the EPRS' author to reiterate the EU's 'We're all in this together' attitude. The EU's policies highlight the aim of addressing the digital divide to ensure that all regions benefit from the positive impacts of digital technologies. This functions as an instrument to simultaneously advance the EU's norms and values regarding multilateralism, human rights, democracy, and social inclusion.[276]

The EU aims to advance its political, economic, and strategic interests while connecting them to "the EU's broader digital, development and security and strategic autonomy agendas."[277] It seeks to establish itself as a strategic player leveraging its expertise and financial resources,[278] with a focus on achieving policy coherence for development and mainstreaming digital technologies in development.[279] Respect for the EU's autonomy in decision-making is crucial.[280]

The EU aims to develop a coherent and global approach for cyber capacity building, "which on one side brings together technology, policy and skills development within a

[271] General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 2.
[272] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 4.
[273] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 14.
[274] Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 2.
[275] Lațici, 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence', 3.
[276] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 2–3.
[277] General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 6.
[278] Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 6.
[279] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 7; European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 7.
[280] General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 5.

broader and overreaching EU development and security agenda, and on other side facilitates the design of an effective EU model for cyber capacity building."[281] Within this framework, cybersecurity is primarily focused on protecting against "malicious cyber activities" targeting digital infrastructure. Thus, it is important to development the necessary capacities to facilitate cybersecurity challenges, mitigate the negative effects of cybercrime,[282] and leverage the full potential of cyber opportunities.[283]

These interpretations indicate a strong emphasis on the importance of taking action for development. Development is necessary, as "a secure and safe digital environment is a necessary condition for reaping the benefits of ubiquitous access to the Internet and the positive effect it has on economic and social development."[284] A key component of development goals is increasing "resilience"[285] and tackling the digital divide.[286] The EU sets a particular focus on Africa, and especially priority countries identified in the *European Agenda on Migration*.[287] Development in the field of cybersecurity integrated various dimensions, aiming for a multifaceted and human-centric understanding of security in digital space.

First, CCB is frequently related to international cooperation, with the EU emphasising the focus on partnerships rather than hierarchical dependencies.[288] Given that cyber issues are seen as global, especially at the threat level, they need to be addressed at the global level.[289] Multistakeholderism and multilateralism are the foundational principles,[290]

[281] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 10.
[282] European Commission, 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 1; General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 6.
[283] Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 2; European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 13.
[284] Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 2.
[285] Presidency of the Council of the European Union, 2.
[286] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 4.
[287] European Commission, 4.
[288] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 8; European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 9.
[289] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 3.
[290] General Secretariat of the Council, 5; General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 2.

involving actors such as UN GGE, OSCE, NATO, WTO, G20, ENISA, GFCE, Europol, as well as academia, civil society, and the private sector.[291] Additionally, bilateral dialogues with strategic partners[292] are effective tools as well. International cooperation facilitates information sharing, exchange of best practices, and joint incident management[293] and is seen to enhance cyber resilience for partner countries.[294] However, this framing indicates a top-down approach.

Likewise, the existing international laws and conventions form the foundation of the international system for the EU. Therefore, relying on international legal action and regulatory frameworks is considered one of the most effective possible solutions to help mitigate the risks of cyberspace and cybersecurity.[295] In terms of CCB, it is thus important to support the implementation of international laws, improving law enforcement, and supporting criminal justice authorities in third countries.[296]

The technological framing advances the use and development of technologies, such as ICTs, as a solution to development issues. Connectivity is seen as an important element of making digital technologies and the digital economy more accessible.[297] The EU sees technologies as a big opportunity for achieving SDGs, inclusive growth, democracy, equality, transparency and empowerment.[298] Potential development solutions may be new

[291] Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 6; General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 6; General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 5; General Secretariat of the Council, 'Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text', 8; General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 11; European Commission, 'Shaping Europe's Digital Future', 13.
[292] General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 11.
[293] Presidency of the Council of the European Union, 'Cyber Capacity Building: Towards a Strategic European Approach', 3.
[294] Collett and Barmpaliou, Panagiota-Nayia, 'International Cyber Capacity Building: Global Trends and Scenarios. Annex 3. Notes on Cyber Capacity Building Funders', 6.
[295] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 6; General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 5; General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 8.
[296] Collett and Barmpaliou, Panagiota-Nayia, 'International Cyber Capacity Building: Global Trends and Scenarios. Annex 3. Notes on Cyber Capacity Building Funders', 6.
[297] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 16.
[298] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 2; European Commission, 'Commission Staff

technological innovations such as 5G and artificial intelligence.[299] Technology is considered helpful in addressing humanitarian issues, managing disasters, and handling migration flows, if privacy is ensured. The framing of technology within development aims to highlight its potential for big societal impact.

In the context of economic growth**,** cybercrime and the lack of global cybersecurity are seen as a risk for the benefits of ICTs, the digital economy, and ultimately the fight against poverty.[300] ICTs are considered an enabler for driving innovation, progress, and development worldwide.[301] Ensuring robust cybersecurity measures is vital for sustaining economic activities, protecting intellectual property, and fostering innovation. The EU's approach emphasises the role of cybersecurity in non-military contexts, highlighting its importance for economic resilience and stability.[302] Fostering sustainable development and economic growth, in general, are the undisputed objectives of development.[303] Economic inclusion should be made accessible for rural areas to reach the goal of eradicating poverty, particularly in Africa.[304]

One of the four main priorities in Digital4Development is to support digital entrepreneurship, start-ups, and small and medium-sized enterprises to create jobs and spur growth while removing barriers to economic development.[305] The private sector, its developments, investments, and access to finance are crucial components, and promoting public-private partnerships is recommended.[306] The EU aims to integrate developing countries

Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 2; European Commission, 5.

[299] General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 5.

[300] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 6; European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 17.

[301] General Secretariat of the Council, 'Council Conclusions on Cyber Diplomacy', 10.

[302] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 2–3.

[303] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 2.

[304] European Commission, 7; European Commission, 17.

[305] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 4; General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 2.

[306] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 6; General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 3.

into the global value chain.[307] To serve the EU's interests, the promotion of the EU's Digital Single Market in its foreign policies is vital. The EU aims to foster international digital trade through common national regulatory frameworks in partner countries,[308] indicating a belief in the 'Brussels Effect' and the top-down approach, while trying to highlight the benefits for local economies.

This connects to political efforts that aim to develop and promote "appropriate frameworks for mainstreaming digital technologies."[309] Development actors should contribute to the establishment of digital policy and regulatory frameworks. Political action has the potential to contribute to digital development and the SDGs. International policy harmonisation is one of the EU's main goals.[310] These legal, policy, or technical frameworks are considered essential for increased resilience.[311] Policy alignment between the EU and Africa is seen as mutually beneficial and an opportunity to develop better business relationships "in the fast growing [sic!] markets of the developing world, based on co-development and co-innovation."[312] This approach links the adaptation of EU standards in third countries to a benefiting economy of these partner countries.

E-Government and digital public services, such as the electronic ID, are another political purpose of development. They aim to enhance effectiveness, accountability, accessibility, and democratic participation in public and administrative services while also preventing fraud.[313] Digital technologies can help realise the "human right to birth registration and nationality," and facilitate humanitarian projects, migration, and refugee management.[314] The EU supports the implementation of digital identification, civil register systems, and the use of biometric measures, and aims to enhance cooperation with partner countries in these areas. Digital civil registration databases are seen as "extremely beneficial" for the

[307] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 6.
[308] General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 5.
[309] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 4.
[310] European Commission, 6–9.
[311] European Commission, 12–13.
[312] European Commission, 15.
[313] European Commission, 14; European Commission, 19–20; General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 4.
[314] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 3.

local population as they contribute to social inclusion. However, it is also mentioned that the implementation of databases in partner countries can support cooperation with the EU on managing legal migration and combating human trafficking in countries of origin.[315] Even if the EU highlights the perceived benefits for local administrations, it cannot ignore its own overriding interests in terms of migration.

The ethical and human rights dimension is a crucial aspect of appropriate development, economic, and political efforts. The free flow of information, freedom of speech, and the right to privacy are fundamental rights for the EU that are urged to be respected. These rights are seen to not only contribute to the ethical use of technologies but can also stimulate economic development and innovation. Acts such as surveillance, censorship, tracking, and other forms of cyberspace "misuse" are considered unethical for the EU and are recognised as threats in the EU Human Rights Guidelines on Freedom of Expression Online and Offline.[316] The EU assumes a monitoring role in this regard to assess the level of compliance.[317] Social media, for example, is viewed as a tool that can help hold governments accountable for human rights violations.[318] Private companies are also identified as having social responsibilities in the digital technologies and solutions they provide.[319]

However, cyber capacity building is seen to have even more benefits for the social aspect of digital transformation. Technology has the potential to enhance social benefits and skills. The growing dependence on ICTs highlights the intertwined nature of social and economic dimensions in cybersecurity. ICTs can have a huge potential for the empowerment of individuals and democracies, serving as tools for socio-economic development and societal progress.[320] Promoting digital skills and literacy is one of the four key priorities in Digital4Development. The "Digital4…" initiative includes various social

[315] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 22.
[316] European Commission, 12.
[317] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 16.
[318] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 19–20.
[319] European Commission, 13.
[320] European Commission, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 2.

dimensions as nexuses,[321] such as education, health, and gender equality. The EU recognises the digital divide as a barrier to inclusive progress and sustainable development. Therefore, it focuses on making broadband connectivity accessible for everyone, especially for rural areas.[322]

Special concerns include the gender digital divide, as well as the economic, political, and social empowerment of marginalised communities such as women, youth, people with disabilities, and those living in remote rural areas. Integrating marginalised groups, especially women, into the IT sector and thereby enabling them to "reap the benefits" of digital transformation can be impeded by socio-cultural constraints.[323] The EU believes that ICTs have the potential to "amplifying women's voices" and break up patterns of inequality.[324] Digital technologies are also seen as a potential strategic enabler for the growth and development of the cultural and creative industry sector with the potential to promote cultural diversity.[325]

In summary, the most frequently mentioned frame is the developmental frame. In addition, the focus was on the social, economic, international cooperation, and technological frame. The legal/regulatory, ethical/human rights, and security frame were mentioned somewhat less frequently. The political, cultural, and geopolitical frame were only mentioned a few times.

Based on these results, I conclude that the EU follows a comprehensive approach dimension to cybersecurity and CCB, covering political, economic, social, and cultural aspects. This includes the emphasis on international cooperation and alliances to foster global cybersecurity. The EU recognises global inequalities and cybersecurity deficiencies as a problem for creating a stable, peaceful international system based on sustainable

[321] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 22–23.
[322] European Commission, 5; European Commission, 11.
[323] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 4; General Secretariat of the Council, 'Digital for Development (D4D) - Council Conclusions (20 November 2017)', 3; General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 2.
[324] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 14.
[325] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 4; European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 9.

development, democracy, and social equality. To address these issues, the EU aims to improve digital infrastructure, technological capabilities, and the minimum standard of cybersecurity. Essentially, development is viewed as the overarching solution for addressing and targeting multifaceted issues in politics, society, and economy. This approach also involves suggesting the activation of "local 'expert' hubs"[326] and that "digital innovation could bring new solutions to local problems."[327] This indicates a top-down framework and yet relates to the local level.

However, one statement that points to a truly more diversified perspective is that the EU also promotes South-South, interregional, and triangular cooperation.[328] An issue that is also sometimes mentioned is the fact that software and the online space are hardly ever developed in "local languages," which is why a multilingual Internet is an essential part of cultural diversity and ownership and should thus be supported.[329]

It seems like the EU's rhetoric implies that global development will lead to an overall improvement of the world. However, it is clear the EU's own interests also come into play, for example concerning migration management outside of the EU's borders. The EU also emphasises its own interests by seeing digital transformation as an opportunity to employ "'Made-in-Europe' solutions" to "help address the needs of developing countries […] as well as create opportunities for European companies to extend their presence in new markets" – resulting in a "win-win" situation.[330]

7. Discussion

The European Union positions itself as a global actor in cyberspace, aspiring to uphold security, prosperity, democracy, and a rules-based international order. However, upon closer examination, there are underlying tensions and contradictions that raise questions about the consistency and coherence of these strategies. This discussion moves beyond

[326] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 13.
[327] European Commission, 6.
[328] General Secretariat of the Council, 'EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)', 10.
[329] General Secretariat of the Council, 'Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)', 6.
[330] European Commission, 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy', 15.

the frame analysis and provides an analysis of these tensions as well as the implications of global power dynamics in the EU's cyber capacity building efforts.

The EU places a strong emphasis on promoting human rights, privacy, and fundamental freedoms in cyberspace. However, its policies also reveal a strong geopolitical agenda. The EU's security and cyber diplomacy strategies are designed to assert its influence and safeguard its strategic interests. Cybersecurity is framed as a shared threat and as a core component of the EU's autonomy of decision and action. This dual approach can lead to contradictions in its policies. For example, while promoting a rules-based global order and human rights, the EU also pursues technological sovereignty and strategic autonomy, which may conflict with its stated goals of multilateralism and cooperation.

The pursuit of strategic partnerships and alliances with 'like-minded countries' is used to enhance the EU's geopolitical position. On the one hand, this approach aligns with the promotion of international cooperation, but on the other hand, it raises critical questions about what defines a 'like-minded country.' As indicated in the literature study, in practice CCB mainly targets countries in the Global South, especially in Latin America and Africa. The EU seeks to persuade them to adopt its norms, values, and solutions. However, when it comes to establishing genuine and more extensive partnerships on eye-level, the EU tends to focus more on countries of the Global North. This creates inconsistency and undermines credibility.

The EU's approach to international cyber policy oscillates between realist and idealist perspectives. The EU employs military and deterrence rhetoric, reflecting concerns about power political and the need to strengthen its own strategic position to safeguard its security as well as its political, strategic, and economic interests. It aims to balance this realist assessment of the strategic environment with an idealist vision and normative aspirations for a better world. The EU seeks to be a global player by advocating for a cyberspace governed by international norms, ethical behaviour, and respect for human rights, which it sees as universal and in everyone's interest. However, non-European actors criticise this universalism, arguing that these 'universal' concepts are rooted in European philosophy and a Eurocentric thinking about the world.

The EU's internal solidarity framework is robust, emphasising the interconnectedness of internal and external security, and the need for a coordinated response to cyber threats. However, external solidarity is less pronounced. While the EU advocates for international cooperation and solidarity, its actions often prioritise its own security and strategic interests. Maintaining a balance between internal and external solidarity is crucial for the EU to be seen as a global leader committed to collective security and development.

The EU's ambition to be a significant cyber player becomes evident in its global strategies and diplomatic efforts. However, my analysis leads to questions about whether the EU has the necessary capacities to meet its ambitions. The reliance on strategic partnerships, the pursuit of technological sovereignty, and the concerns about external dependencies highlight potential vulnerabilities. The EU's emphasis on building a robust and cooperative defence industry underscores its recognition of the need to enhance internal capacity to achieve its strategic goals.

My critical analysis of the EU's CCB efforts reveals potential neocolonial undertones. Despite promoting equal partnerships and cooperation, South-South capacity building and local ownership, the EU's approach tends to reinforce asymmetric power relations. Through my analytical lens, the emphasis on "European solutions," "our technology," and the promotion of EU standards and values can be interpreted as a continuation of the EU's historical dominance. Local agency and solutions are overshadowed by European interests as the EU seeks to assert its role in a "scramble" for the emerging markets in the Global South. The advertised technologies and frameworks are developed outside the local context, which does not allow for a shift in the autonomy and agency of local actors. This raises concerns about the effective inclusivity and equity of the EU's capacity building initiatives and risks creating dependencies on European technologies and expertise rather than fostering genuine self-sufficiency. Instead, the goal to improve resilience is reiterated frequently, but often lacks precise definition and contextual clarity. This may obscure substantive structural changes.

As my findings suggest, the emphasis on "local ownership" can become a token gesture if not accompanied by sincere efforts to involve local stakeholders in the decision-making process and tailor solutions to their specific needs and contexts – not just in words, but in actions as well. Additionally, the aspect of administration and registration of people in

Global South countries has a significant colonial component and may once again be rooted in Europe's interest to establish a specific form of order and governance and manage migration outside the EU's borders.

By implicitly or explicitly positioning itself as the provider of technological and developmental solutions to the Global South, the EU reinforces a dichotomy between the 'developed' North and the 'underdeveloped' South. This dynamic positions Southern countries as (passive) recipients of Northern benevolence, perpetuating historical patterns of dependency and control. As De Roeck, Delputte, and Orbie note, this approach risks replicating colonial power structures under the guise of resilience and capacity building.[331] Instead of moving to eye-level, the EU spirals back into traditional, unequal development paradigms.

The EU promotes digital technologies as a panacea for a wide range of issues, from economic development to social inclusion. This indicates a tendency towards techno-solutionism, which is the belief that technological innovation can solve complex social problems. Techno-solutionist ideas oversimplify the role of technology in development and overlook the social, economic, and cultural factors at play. It embraces the belief that technological advancement is the ultimate catalyst for growth and progress, resulting in an improved quality of life. However, this linear and idealised notion of progress has its origins in colonialism, and it is rooted in a top-down Eurocentric perception of non-European societies and cultures. Relying so strongly on digital technologies for development fails to capture a nuanced vision of society and consider potential limitations and risks associated with the digital transformation.

The EU's core value regarding digital technologies is to promote data protection, privacy, and fundamental rights online. The EU recognises the risks of unethical misuse of digital tools, such as surveillance and digital control, which can potentially infringe on individual rights. This risk is particularly positioned in so-called authoritarian und undemocratic regimes. However, this collides with reality. Firstly, the EU presents biometric and registration technologies as a tool to manage humanitarian issues and migration flows if it is in its own interests, disregarding significant ethical concerns and risks. This particularly

[331] De Roeck, Delputte, and Orbie, 'Framing the Climate-Development Nexus in the European Union', 10.

applies to undocumented refugees and the potential misuse of European technologies in partner countries. Secondly, EU member states are also known to use digital tools for political purposes and to increase digital surveillance, for example in public spaces or border control, usually justified in the name of combating 'terror.'

The EU's approach to cybersecurity and digital governance is fragmented, with competing priorities and inconsistent policy implementation, reducing its effectiveness. The focus on technological sovereignty and strategic autonomy can conflict with the goal of promoting a global, open, and secure cyberspace. The EU's efforts to project its values and standards globally are undermined by its inward-looking strategies, which prioritise European interests over genuine solidarity. The tension between geopolitical and normative objectives, coupled with the potential neocolonial undertones in its capacity building efforts, presents significant challenges for the EU's credibility as a global leader in cyberspace.

8. Conclusion

This thesis has explored how the EU positions itself as a contemporary global development actor in the field of international cybersecurity. Drawing on concepts from international development, cyber governance, international cybersecurity and the EU's global actorness, I have examined how the EU frames cyber capacity building. Through frame analysis, I have gained nuanced insights into how these issues are constructed, which problems and solutions are presented, and how the EU positions itself in addressing these issues. By adopting a Global Studies approach, this research contributes to our critical understanding of cybersecurity as an issue in global politics and adds to the political and social science literature on cybersecurity. In the following, I address my research questions, confirming my hypothesis about the EU's strategic approach to cyberspace and my main argument about the colonial continuity of the EU's global position, including in the field of cybersecurity.

The EU frames cybersecurity and CCB within a multifaceted, human security but also geopolitical narrative. This strategy is rooted in normative values, geopolitical concerns, and economic growth. The EU emphasises the need for international cooperation based on the European ideas of democracy and human rights. Norms, deterrence, and

entanglement through strategic alliances all appear as strategies to ensure a more stable cyberspace. Cybersecurity is presented as critical not only for protecting data and infrastructure but also for advancing global stability and prosperity. This raises its significance to the level of global importance for the whole of society, with 'developing countries' being particularly vulnerable to threats. The EU's approach to CCB is seen to improve societal well-being, bolster global cyber resilience, reduce digital divides, and promote sustainable development through technological solutions, while also serving as a tool for diplomatic engagement and geopolitical strategy.

The EU's role as a global digital actor and its activities in the field of digital development are significantly influenced by postcolonial structures and Eurocentric ideologies. Its strategies mostly implicitly, and sometimes even explicitly, reflect a continuum of historical dynamics and worldviews based on the coloniality of power, where European norms and standards are promoted as the benchmark for global practices. This approach carries the risk of creating new dependencies and perpetuating global inequalities, as it positions the EU as a provider of technology and knowledge. While the EU emphasises its new, egalitarian approach to development based on partnerships and cooperation, these efforts can conceal underlying asymmetries in power and influence, remnants of colonial relations.

The EU prominently promotes a human-centric digital transformation. However, its CCB initiatives also serve broader strategic and geopolitical agendas. These include countering the influence of other global powers like China and Russia, which are not considered like-minded, as well as enhancing its digital sovereignty, and securing its geopolitical position through strategic alliances and increased autonomy. Therefore, the EU's human-centric rhetoric is often driven by strategic interests, indicating a dual motivation in its international digital policy.

However, rather than establishing a binary between the geopolitical and the normative, the combination of both concerns in EU policy shows how the EU seeks to create its sense of identity in a changing post-colonial world order, navigating the geopolitical realities of the digital 21st century. In short, the geopolitical elements aim to reestablish and maintain power positions rooted in colonial times, while the normative agenda aims to create

a uniqueness and distinction from other international actors, with technology being one of the tools.

Whilst this study has contributed an interdisciplinary political perspective to the study of cybersecurity, there have been limitations to the research. It is important to reiterate that my positionality is located within the EU. My work draws on excellent research and critical analyses of scholars, who are predominantly situated in the Global North as well. Future studies could add to my analysis by expanding the scope of the research, for example by including perspectives and interpretations from the Global South. My interpretations are based on my subjective understanding, so different scholars will likely arrive at different results. Similarly, examining the practical actions of the EU in the field, for example through expert interviews or participant observation, could provide a more holistic understanding of interventions and impacts on the ground. Additionally, future research could delve into the impact of colonial legacies on domestic EU digital policies, further analyse the 'Brussels Effect,' or conduct a postcolonial analysis of digital sovereignty. The implications of this study serve as a starting point for providing insights into critical EU studies in a policy domain of growing global significance that has not received much attention yet.

9. Bibliography

Amazouz, Souhila. ‘Cyber Capacity-Building and International Security’. In *Routledge Handbook of International Cybersecurity*, edited by Eneken Tikk and Mika Kerttunen, 201–13. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2020.

Arnold, David. ‘Europe, Technology, and Colonialism in the 20th Century’. *History and Technology* 21, no. 1 (March 2005): 85–106. https://doi.org/10.1080/07341510500037537.

Barbero, Fabio, and Nils Berglund. ‘Cybersecurity Capacity Building and Donor Coordination in the Western Balkans’. Geneva Centre for Security Sector Governance, 2021.

Barrinha, André, and Thomas Renard. ‘Cyber-Diplomacy: The Making of an International Society in the Digital Age’. *Global Affairs* 3, no. 4–5 (20 October 2017): 353–64. https://doi.org/10.1080/23340460.2017.1414924.

Bartlett, Benjamin. ‘Why Do States Engage in Cybersecurity Capacity-Building Assistance? Evidence from Japan’. *The Pacific Review* 37, no. 3 (3 May 2024): 475–503. https://doi.org/10.1080/09512748.2023.2183242.

Blaut, J. M. *The Colonizer’s Model of the World: Geographic Diffusionism and Eurocentric History.* New York, London: The Guilford Press, 2012.

Calandro, Enrico, and Nils Berglund. ‘Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case’. Berlin, 2019. https://www.giganet.org/2019symposiumPapers/33_Calandro_Berglund_Unpacking%20Cyber-Capacity%20Building.pdf.

Calderaro, Andrea, and Anthony J. S. Craig. ‘Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building’. *Third World Quarterly* 41, no. 6 (2 June 2020): 917–38. https://doi.org/10.1080/01436597.2020.1729729.

Carver, Julia. ‘More Bark than Bite? European Digital Sovereignty Discourse and Changes to the European Union’s External Relations Policy’. *Journal of European Public Policy*, 2 January 2024, 1–37. https://doi.org/10.1080/13501763.2023.2295523.

Cervi, Giulio Vittorio. ‘Why and How Does the EU Rule Global Digital Policy: An Empirical Analysis of EU Regulatory Influence in Data Protection Laws’. *Digital Society* 1, no. 2 (September 2022): 18. https://doi.org/10.1007/s44206-022-00005-3.

Chiappetta, Andrea. ‘The Cybersecurity Impacts on Geopolitics’. *Formamente* XIV, no. 1/2019 (2019): 61–74.

Christou, George, and Seamus Simpson. ‘The European Union, Multilateralism and the Global Governance of the Internet’. *Journal of European Public Policy* 18, no. 2 (March 2011): 241–57. https://doi.org/10.1080/13501763.2011.544505.

Claessen, Eva. ‘Reshaping the Internet – the Impact of the Securitisation of Internet

Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU'. *Journal of Cyber Policy* 5, no. 1 (2020): 140–57. https://doi.org/10.1080/23738871.2020.1728356.

Collett, Robert. 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures'. *Journal of Cyber Policy* 6, no. 3 (2 September 2021): 298–317. https://doi.org/10.1080/23738871.2021.1948582.

Collett, Robert, and Barmpaliou, Panagiota-Nayia. 'International Cyber Capacity Building: Global Trends and Scenarios. Annex 3. Notes on Cyber Capacity Building Funders'. European Commission, September 2021.

Cooper, Frederick, and Randall Packard. 'Introduction'. In *International Development and the Social Sciences. Essay on the History and Politics of Knowledge.*, edited by Frederick Cooper and Randall Packard, 1–41. Berkeley, Los Angeles, London: University of California Press, 1997.

Council of Europe. 'Chart of Signatures and Ratifications of Treaty 185'. Council of Europe Treaty Office. Accessed 12 August 2024. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

Craig, Anthony J. S., Richard A. I. Johnson, and Max Gallop. 'Building Cybersecurity Capacity: A Framework of Analysis for National Cybersecurity Strategies'. *Journal of Cyber Policy* 7, no. 3 (2 September 2022): 375–98. https://doi.org/10.1080/23738871.2023.2178318.

Creese, Sadie, William H. Dutton, Patricia Esteve-González, Michael Goldsmith, Eva Nagyfejeo, Jamie Saunders, Basie Von Solms, and Carolin Weisser Harris. 'The Solution Is in the Details: Building Cybersecurity Capacity in Europe'. *SSRN Electronic Journal*, 2022. https://doi.org/10.2139/ssrn.4178109.

Darian-Smith, Eve, and Philip C. McCarty. 'Why Is Global Studies Important?' In *The Global Turn: Theories, Research Designs, and Methods for Global Studies*, 29–54. Berkeley: University of California Press, 2017.

De Roeck, Frederik, Sarah Delputte, and Jan Orbie. 'Framing the Climate-Development Nexus in the European Union'. *Third World Thematics: A TWQ Journal* 1, no. 4 (3 July 2016): 1–17. https://doi.org/10.1080/23802014.2016.1286947.

Deibert, Ronald. 'Cyber-Security'. In *Routledge Handbook of Security Studies*, edited by Thierry Balzacq and Myriam D. Cavelty, 2nd ed., 314–32. Abingdon, Oxon; New York, NY: Routledge, 2017.

Delputte, Sarah, and Jan Orbie. 'Paradigm Shift or Reinventing the Wheel? Towards a Research Agenda on Change and Continuity in EU Development Policy'. *Journal of Contemporary European Research* 16, no. 2 (16 June 2020). https://doi.org/10.30950/jcer.v16i2.1084.

DeNardis, Laura. 'The Emerging Field of Internet Governance'. In *The Oxford Handbook of Internet Studies*, edited by William H. Dutton, 555–76. Oxford University Press, 2013.

https://doi.org/10.1093/oxfordhb/9780199589074.013.0026.

Directorate-General for International Partnerships. 'DG International Cooperation and Development Becomes DG International Partnerships'. European Commission, 15 January 2021. https://international-partnerships.ec.europa.eu/news-and-events/news/dg-international-cooperation-and-development-becomes-dg-international-partnerships-2021-01-15_en.

Doidge, Mathew, and Martin Holland. 'A Chronology of European Union Development Policy: Theory and Change'. *Korea Review of International Studies* 17, no. 1 (2015): 59–80.

Dunn Cavelty, Myriam. 'Cybersecurity between Hypersecuritization and Technological Routine'. In *Routledge Handbook of International Cybersecurity*, edited by Mika Kerttunen and Eneken Tikk, 11–21. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2020.

———. 'Europe's Cyber-Power'. *European Politics and Society* 19, no. 3 (27 May 2018): 304–20. https://doi.org/10.1080/23745118.2018.1430718.

Dunn Cavelty, Myriam, and Andreas Wenger. 'Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science'. *Contemporary Security Policy* 41, no. 1 (2 January 2020): 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Dutton, William H., Sadie Creese, Ruth Shillair, and Maria Bada. 'Cybersecurity Capacity. Does It Matter?' *Journal of Information Policy* 9 (2019): 280–306.

Dwyer, Andrew C, Clare Stevens, Lilly Pijnenburg Muller, Myriam Dunn Cavelty, Lizzie Coles-Kemp, and Pip Thornton. 'What Can a Critical Cybersecurity Do?' *International Political Sociology* 16, no. 3 (23 July 2022): 1–26. https://doi.org/10.1093/ips/olac013.

Erforth, Benedikt, and Charles Martin-Shields. 'Where Privacy Meets Politics: EU-Kenya Cooperation in Data Protection'. In *Africa–Europe Cooperation and Digital Transformation. Innovations in International Affairs*, edited by Benedikt Erforth, Chloe Teevan, and Chux Daniels. Milton Park, Abingdon, Oxon; New York, NY: Routledge, Taylor & Francis Group, 2023.

EU CyberNet. 'Mapping of EU-Funded External Cyber Capacity Building Actions 2022'. European Commission, 2022.

European Commission. 'Commission Staff Working Document. Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy'. Brussels, 2 May 2017.

———. 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'. Brussels, 7 February 2013. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001.

———. 'EU Cybersecurity Initiatives Working towards a More Secure Online

Environment - Factsheet'. Brussels, January 2017.

———. 'Report on Implementation of the EU's Cybersecurity Strategy for the Digital Decade'. Brussels, 23 June 2021.

———. 'Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU'. Brussels, 13 September 2017.

———. 'Shaping Europe's Digital Future'. Brussels, 19 February 2020.

———. 'The European Agenda on Security'. Strasbourg, 28 April 2015.

———. 'The EU's Cybersecurity Strategy for the Digital Decade'. Brussels, 16 December 2020.

European Parliament, European Commission, and Council of the European Union. 'The New European Consensus on Development: "Our World, Our Dignity, Our Future"'. Official Journal of the European Union, 30 June 2017.

European Union. 'A Global Strategy for the European Union's Foreign And Security Policy', June 2016.

———. 'Operational Guidance for the EUs International Cooperation on Cyber Capacity Building'. Luxembourg: Publications Office, 2018.

European Union Agency for Cybersecurity. 'About ENISA - The European Union Agency for Cybersecurity'. European Union Agency for Cybersecurity. Accessed 12 August 2024. https://www.enisa.europa.eu/about-enisa.

Finnemore, Martha, and Duncan B. Hollis. 'Constructing Norms for Global Cybersecurity'. *American Journal of International Law* 110, no. 3 (July 2016): 425–79. https://doi.org/10.1017/S0002930000016894.

Flick, Uwe, Ines Steinke, and Ernst von Kardorff. 'What Is Qualitative Research? An Introduction to the Field'. In *A Companion to Qualitative Research*, edited by Uwe Flick, Ines Steinke, and Ernst von Kardorff, translated by Bryan Jenner, 3–12. London, Thousand Oaks, New Delhi: SAGE Publications, 2004.

Flint, Colin. *Introduction to Geopolitics*. London; New York: Routledge, 2006.

Fritzsche, Kerstin, and Daniel Spoiala. 'The EU-AU Digital Partnership'. In *Africa–Europe Cooperation and Digital Transformation. Innovations in International Affairs*, edited by Chux Daniels, Chloe Teevan, and Benedikt Erforth, 17–31. Milton Park, Abingdon, Oxon; New York, NY: Routledge, Taylor & Francis Group, 2023.

General Secretariat of the Council. 'A Strategic Compass for Security and Defence - For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security'. Brussels: Council of the European Union, 21 March 2022.

———. 'Council Conclusions on Cyber Diplomacy'. Brussels: Council of the European

Union, 11 February 2015.

———. ‘Council Conclusions on EU Digital Diplomacy - Council Conclusions’. Brussels: Council of the European Union, 26 June 2023.

———. ‘Council Conclusions on the EU Policy on Cyber Defence’. Brussels: Council of the European Union, 22 May 2023.

———. ‘Council Conclusions on the Future of Cybersecurity: Implement and Protect Together’. Brussels: Council of the European Union, 21 May 2024.

———. ‘Digital for Development (D4D) - Council Conclusions (20 November 2017)’. Brussels: Council of the European Union, 20 November 2017.

———. ‘Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities - Approval of the Final Text’. Brussels: Council of the European Union, 9 October 2017.

———. ‘EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)’. Brussels: Council of the European Union, 26 June 2018.

———. ‘Mainstreaming Digital Solutions and Technologies in EU Development Policy - Council Conclusions (28 November 2016)’. Brussels: Council of the EUropean Union, 28 November 2016.

Grigsby, Alex. ‘The End of Cyber Norms’. *Survival* 59, no. 6 (2 November 2017): 109–22. https://doi.org/10.1080/00396338.2017.1399730.

Hansen, Peo, and Stefan Jonsson. ‘Bringing Africa as a “Dowry to Europe”: European Integration and the Eurafrican Project, 1920–1960’. *Interventions* 13, no. 3 (September 2011): 443–63. https://doi.org/10.1080/1369801X.2011.597600.

Hohmann, Marko, Alexander Pirang, and Throsten Benner. ‘Advancing Cybersecurity Capacity Building. Implementing a Principle-Based Approach.’ Edited by Global Public Policy Institute, March 2017.

Homburger, Zine. ‘The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace’. *Global Society* 33, no. 2 (3 April 2019): 224–42. https://doi.org/10.1080/13600826.2019.1569502.

Hurel, Louise Marie. ‘Interrogating the Cybersecurity Development Agenda: A Critical Reflection’. *The International Spectator* 57, no. 3 (2022): 66–84. https://doi.org/10.1080/03932729.2022.2095824.

Izycki, Eduardo, Brett Van Niekerk, and Trishana Ramluckan. ‘Cyber Diplomacy: NATO/EU Engaging with the Global South’. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 417–35. Tallinn, Estonia: IEEE, 2023. https://doi.org/10.23919/CyCon58705.2023.10182095.

Kerttunen, Mika, and Tikk Eneken. ‘The Politics of Stability. Cement and Change in

Cyber Affairs'. In *Routledge Handbook of International Cybersecurity*, edited by Mika Kerttunen and Tikk Eneken, 52–64. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2020.

Kumar, Yogendra. *Geopolitics in the Era of Globalisation. Mapping an Alternative Global Future*. Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2021.

Kurbalija, Jovan. *An Introduction to Internet Governance*. 7th edition. Msida, Malta Geneva Belgrade: DiploFoundation, 2016.

Lațici, Tania. 'Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence'. Brussels: European Parliament, May 2020.

Lindekilde, Lasse. 'Discourse and Frame Analysis: In-Depth Analysis of Qualitative Data in Social Movement Research'. In *Methodological Practices in Social Movement Research*, edited by Donatella della Porta, 195–227. Oxford: Oxford University Press, 2014.

Mărcuț, Mirela. 'Evaluating the EU's Role as a Global Actor in the Digital Space'. *Romanian Journal of European Affairs* 20, no. 2 (December 2020): 79–85.

Marx, Leo, and Merritt Roe Smith. *Does Technology Drive History?: The Dilemma of Technological Determinism*. Edited by Leo Marx and Merritt Roe Smith. Cambridge, Massachusetts, London, England: MIT Press, 1994.

Mason, Mike. *Global Shift. Asia, Africa, and Latin America, 1945-2007*. Montreal, Kingston, London, Ithaca: McGill-Queen's University Press, 2013.

Middell, Matthias. 'What Is Global Studies All About?' *Global Europe – Basel Papers on Europe in a Global Perspective*, no. 105 (2014): 38–49.

Monsees, Linda, and Daniel Lambach. 'Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity'. *European Security* 31, no. 3 (3 July 2022): 377–94. https://doi.org/10.1080/09662839.2022.2101883.

Muller, Lilly Pijnenburg. 'Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities'. Policy Brief. NUPI Report. Oslo: NUPI, 2015.

Mumford, Densua, and James Shires. 'Toward a Decolonial Cybersecurity: Interrogating the Racial-Epistemic Hierarchies That Constitute Cybersecurity Expertise'. *Security Studies*, 25 September 2023, 1–31. https://doi.org/10.1080/09636412.2023.2230879.

O'Hara, Kieron, Wendy Hall, and Vinton Cerf. *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. Oxford: Oxford University Press, 2021.

Orbie, Jan. 'International Development. A Distinct and Challenged Policy Domain'. In *Policy-Making in the European Union*, edited by Helen Wallace, Mark A. Pollack, Christilla Roederer-Rynning, and Alasdair R. Young, 8th ed., 413–39. Oxford: Oxford University Press, 2020. https://doi.org/10.1093/hepl/9780198807605.001.0001.

———. 'The EU's Role in Development: A Full-Fledged Development Actor or Eclipsed

by Superpower Temptations?' In *The European Union and Global Development*, edited by Stefan Gänzle, Sven Grimm, and Davina Makhan, 17–36. London: Palgrave Macmillan, 2012.

———. 'The Graduation of EU Development Studies: Towards a Post-Colonial Turn?' *Global Affairs* 7, no. 4 (8 August 2021): 597–613. https://doi.org/10.1080/23340460.2021.1999175.

Pawlak, Patryk. 'Capacity Building in Cyberspace as an Instrument of Foreign Policy'. *Global Policy* 7, no. 1 (February 2016): 83–92. https://doi.org/10.1111/1758-5899.12298.

———. 'Introduction'. In *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development.*, edited by Patryk Pawlak, 21:9–17. ISSUE. Paris: EU Institute for Security Studies, 2014. https://data.europa.eu/doi/10.2815/43313.

Pawlak, Patryk, and Panagiota-Nayia Barmpaliou. 'Politics of Cybersecurity Capacity Building: Conundrum and Opportunity'. *Journal of Cyber Policy* 2, no. 1 (2 January 2017): 123–44. https://doi.org/10.1080/23738871.2017.1294610.

Presidency of the Council of the European Union. 'Cyber Capacity Building: Towards a Strategic European Approach'. Brussels: Council of the European Union, 30 June 2016.

Przetacznik, Jakub, and Simona Tarpova. 'Russia's War on Ukraine: Timeline of Cyber-Attacks'. Briefing. European Parliamentary Research Service, June 2022.

Quijano, Aníbal. 'Colonialidad del poder, Eurocentrismo y América Latina'. In *La colonialidad del saber: Eurocentrismo y ciencias sociales: Perspectivas latinoamericanas*, edited by Edgardo Lander, 201–46. Buenos Aires: UNESCO, CLASCO, 2000.

Renard, Thomas. 'EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain'. *European Politics and Society* 19, no. 3 (27 May 2018): 321–37. https://doi.org/10.1080/23745118.2018.1430720.

Renda, Kadri Kaan. 'The Development of EU Cybersecurity Policy: From a Coordinating Actor to a Cyber Power?' *Ankara Avrupa Calismalari Dergisi* 21, no. 2 (30 December 2022): 467–95. https://doi.org/10.32450/aacd.1226890.

Said, Edward. *Orientalism*. Minneapolis, USA: Random House, 1979.

Saran, Samir. 'Striving for an International Consensus on Cyber Security: Lessons from the 20th Century'. *Global Policy* 7, no. 1 (February 2016): 93–95. https://doi.org/10.1111/1758-5899.12317.

Savaş, Serkan, and Süleyman Karataş. 'Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance'. *International Cybersecurity Law Review* 3, no. 1 (June 2022): 7–34. https://doi.org/10.1365/s43439-021-00045-4.

Schia, Niels Nagelhus. 'The Cyber Frontier and Digital Pitfalls in the Global South'. *Third World Quarterly* 39, no. 5 (4 May 2018): 821–37. https://doi.org/10.1080/01436597.2017.1408403.

Sebhatu, Rahel Weldeab. ‘Applying Postcolonial Approaches to Studies of Africa-EU Relations’. In *The Routledge Handbook of EU-Africa Relations*, edited by Toni Haastrup, Luís Mah, and Niall Duggan, 38–50. Milton Park, Abingdon, Oxon; New York, NY: Routledge, Taylor & Francis Group, 2021.

Siudak, Robert. ‘Cybersecurity Discourses and Their Policy Implications’. *Journal of Cyber Policy* 7, no. 3 (2 September 2022): 318–35. https://doi.org/10.1080/23738871.2023.2167607.

Sund, Christine. ‘Towards an International Road-map for Cybersecurity’. *Online Information Review* 31, no. 5 (2 October 2007): 566–82. https://doi.org/10.1108/14684520710832306.

Teevan, Chloe. ‘Building Strategic European Digital Cooperation with Africa’. Briefing Note. ecdpm, September 2021.

United Nations General Assembly. ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’, 22 July 2015. https://digitallibrary.un.org/record/799853?v=pdf.

United Nations Office for Disarmament Affairs. ‘Developments in the Field of Information and Telecommunications in the Context of International Security’. *United Nations Office for Disarmament Affairs* (blog). Accessed 12 August 2024. https://disarmament.unoda.org/ict-security/.

Unwin, Tim. ‘Development Agendas and the Place of ICTs’. In *ICT4D: Information and Communication Technology for Development*, edited by Tim Unwin, 7–38. Cambridge, UK: Cambridge University Press, 2009.

Van Hulst, Merlijn, Tamara Metze, Art Dewulf, Jasper De Vries, Severine Van Bommel, and Mark Van Ostaijen. ‘Discourse, Framing and Narrative: Three Ways of Doing Critical, Interpretive Policy Analysis’. *Critical Policy Studies*, 9 April 2024, 1–23. https://doi.org/10.1080/19460171.2024.2326936.

Van Hulst, Merlijn, and Dvora Yanow. ‘From Policy “Frames” to “Framing”: Theorizing a More Dynamic, Political Approach’. *The American Review of Public Administration* 46, no. 1 (January 2016): 92–112. https://doi.org/10.1177/0275074014533142.