Drivers for International Cyber Capacity Building Investments

Tienhoven, Manon van

Drivers for International Cyber Capacity Building Investments

Manon van Tienhoven

Supervisor: Dr. James Shires
Second reader: Dr. Els de Busser

Master Thesis
Cyber Security

Word count: 21.890 words
5 December 2021

Abstract

This study aims to build and expand the academic debate on cyber capacity building (CCB) through analyzing what the drivers are for donor countries to invest in CCB efforts; more specifically, whether the internet governance divisions shape international CCB investment decisions. This study pioneers by attempting to provide empirical evidence on the potential link between CCB as a foreign policy tool and the internet governance debate - a global discussion that demonstrates geopolitical divisions between two conflicting ideologies - multi-stakeholder and a more sovereign approach - on how the internet should be governed. The empirical evidence is gathered through conducting semi-structured interviews with representatives from Australia, Canada, the Netherlands, and the UK, and open-source databases, such as the UN voting records and Cybil – the CCB repository. The empirical findings in this study demonstrate that capacity building investments can be used as a foreign policy tool to promote national interests. However, CCB is just one of the many diplomatic tools available, and the analysis demonstrates that influencing a country's position in the internet governance debate, is never a sole or even a prioritized driver for cyber capacity building investment decisions.

Key words: cyber capacity building, internet governance debate, drivers, foreign policy objectives, investment decisions

Table of Contents

Figures and Tables

Acronyms

ASEAN	Association of Southeast Asian Nations
CCB	Cyber capacity building
CIIP	Critical Information Infrastructure Protection
CSIRT	Computer Security Incident Response Team
EU	European Union
GFCE	Global Forum on Cyber Expertise
ICANN	Internet Corporation for Assigned Names and Numbers
ISOC	Internet Society
ITR	International Telecommunication Regulations
ITU	International Telecommunication Union
LDC	Least Developed Country
NGO	Non-governmental organizations
ODA	Official Development Assistance
OECD	Organization for Economic Co-operation and Development
OEWG	Open-Ended Working Group
SCO	Shanghai Cooperation Organization
SDG	Sustainable Development Goal
UK	United Kingdom
UN	United Nations
UNGA	United Nations General Assembly
UN GGE	United Nations Group of Governmental Experts
US	United States
WGIG	Working Group on Internet Governance

1. Introduction

The rise of the internet has brought many social and economic opportunities, but at the same time, has also brought new challenges and threats posed to governments, companies, and citizens. Presently, there are over 3.5 billion people with access to the internet,[1] which is half of the world's population, and it is unthinkable to have a world without the internet. All countries have been impacted by the opportunities that the internet has to offer. It is a key enabler for the global economy, society, as well as governments; more and more structures are relying on the use of digital systems. Research has demonstrated that access to the internet has a huge influence on developing countries, which can be linked to economic growth, jobs and services.[2] Therefore, it is not surprising, that one of the United Nation's Sustainable Development Goals (SDGs) is focused on increasing the accessibility of Least Development Countries (LDCs) to ICT services and the provision of universal and affordable access to the internet.[3] A lot of progress has been made with regard to LDCs having better access to the internet over the past years. According to the statistics, only 4% of LDCs were connected to the internet back in 2010, compared to 18% in 2017.[4]

Although it is optimistic that the developing countries and LDCs are increasingly getting access to the internet, it also brings along new challenges and threats for countries. Criminals now have a new avenue to conduct illegal activities through the internet, commonly referred to as 'cybercrime' that includes the theft of data and money, fraud, ransomware, disruption of services, to just name a few examples. It is estimated that cybercrime will costs the world's economy by 2025, over $10.5 trillion dollars on an annual basis.[5] Further, other threats can cause harm to a country's cybersecurity that can impact national critical infrastructure, vital industry, or harm individuals. Therefore, cybersecurity can be referred to as the ability to respond to threats.[6] Due to the enormous growth of digitalization, especially in developing

[1] International Telecommunication Union, *Global Cybersecurity Index*, 2020.
[2] The World Bank Group, *Digital Dividends*, 2016.
[3] United Nations, "Transforming Our World: The 2030 Agenda for Sustainable Development," 2015.
[4] The 2017 data is the most recent available data in open source databases as ITU, UN, and the World Bank (November 2021); Andrea Calderaro and Anthony J.S. Craig, "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building," *Third World Quarterly* 41, no. 6 (2020): 917–38, https://doi.org/10.1080/01436597.2020.1729729.
[5] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," accessed October 17, 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
[6] Lilly Pijnenburg Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities," *Norwegian Institute of International Affairs*, no. 3 (2015): 23, https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf.

countries, this also results in an increasing growth of cyber threats. The challenge developing countries face with rapidly becoming connected to the internet is that there is a risk that cybersecurity becomes an afterthought; the priority is getting access to the internet instead of in parallel ensuring the securitization of ICT infrastructure.[7] Due to the lack of cybersecurity, threats can cause more harm to a country and its local economy than the state can benefit from the internet.[8]

Therefore, there is increasingly more attention for 'cyber capacity building' (CCB) on a global political level. International cyber capacity building efforts implies that countries and other stakeholders support each other to develop the necessary national capacities, including functioning and accountable institutions, in order to take action against cybercrime threats and strengthen the cyber resilience of countries.[9] This suggests that cyber capacity building could help countries with their accessibility to the internet as well as to ensure that they are aware and able to respond to cyber threats. There has been a vast increase in the number of cyber capacity building projects targeted at developing countries and LDCs since 2015 by a diverse group of stakeholders, and many of these cyber capacity building activities are funded by 'donor' countries: developed countries that have a relative high level of national cybersecurity.[10]

This raises the question: what is the motivation for those countries that increasingly fund the building of these cyber capacities in developing countries and LDCs? There is academic literature that links donor countries' interest in developing countries to promote their own foreign policy objectives. An example of such foreign policy objectives is linked to the ongoing global internet governance debate;[11] a global discussion that demonstrates geopolitical divisions between two conflicting ideologies - multi-stakeholder and a more sovereign approach - on how the internet should be governed. The literature suggests that cyber capacity building can be used to further foreign policy objectives to sway the recipient countries to the side of the respective

[7] Mirko Hohmann et al., "Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach," *Global Public Policy Institute (GPPi)*, 2017, http://www.gppi.net/fileadmin/user_upload/media/pub/2017/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf.

[8] Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities."

[9] There are different types of cyber capacity building, for example countries also invest in their national domestic capacities. For the purpose of this thesis, cyber capacity building refers to international cyber capacity building efforts, capacity efforts between countries.

[10] Robert Collett and Nayia Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios," 2021, https://doi.org/10.2815/06590.

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

donor in the debate. However, there has been limited empirical research that examines more in-depth what the drivers are of donor countries and their cyber capacity building investments, specifically connecting how this can be used to influence the position of countries in the internet governance debate.

1.1 Research question

This thesis aims to make an attempt to better understand the motivation of donor countries to invest in international cyber capacity building activities and whether this is related to furthering their foreign policy objectives regarding the internet governance debate. Although cyber capacity building is perceived as a form of development aid, it is unclear what the drivers are for countries to link cyber capacity building to their own national priorities and foreign policy objectives. Therefore, this thesis aims to build and expand on the existing academic debate by posing the main research question: *To what extent do internet governance divisions shape international cyber capacity building investment decisions?*

In order to answer the main research question, the thesis is guided by the following four sub-research questions:

1. *What is Cyber Capacity Building and how is it linked to foreign policy objectives?*
2. *What are the internet governance divisions in the international arena?*
3. *Which countries receive cyber capacity support from donor countries?*
4. *What are the motivations of countries to invest in international cyber capacity building activities?*

The hypothesis that will be tested in this study is that: *International cyber capacity building investments are targeted at like-minded countries and digital swing states*. Additionally, the thesis has narrowed down its scope in the following way. First, it will limit its research to the multi-stakeholder camp by examining its cyber capacity activities and its donor countries. Secondly, in order to get a better understanding of foreign policy objectives, the scope is limited to cyber capacity building investments directly from donor countries and will not focus on cyber capacity building investments through international and regional organizations. These delimitations will be further elaborated on in the Research Design section of the study.

1.2 Academic and societal relevance

Cyber capacity building activities are increasing globally, but especially in developing countries, and more and more stakeholders are becoming active in this field.[12] This form of assistance is vital for countries to use the internet in a secure manner that will promote their overall national development and security.[13] Two examples of international cyber capacity efforts are: support with cybercrime legislation or a national cybersecurity assessment; for instance, the Cyber Maturity Model that allows countries to review their level of cyber capacity as well as how to improve it.[14] Yet, although multiple literature refers to the drivers of cyber capacity building,[15] there is little empirical research to support this, for instance from a donor's perspective to what extent their cyber capacity building efforts are linked to their own foreign policy objectives.

Additionally, the internet governance debate is increasing in importance. During the 2021 virtual Munich Security Conference, Joe Biden, President of the United States, Ursula von der Leyen, President of the EU Commission, Emmanuel Macron, President of France, and António Guterres, the Secretary-General of the United Nations, raised the issues related to the Internet as one of the most important challenges for the period post-COVID.[16] The internet governance debate is also ongoing on a global level, for example on the UN level through the United Nations Governmental Group of Experts (UN GGE) and the Open-Ended Working Group (OEWG) processes in which cyber capacity building is also a recurring topic.

Therefore, there is academic relevance for this thesis to examine the motivation of countries to invest in cyber capacity building activities and whether this is linked to the internet governance debate divisions. Hence, this could provide new insights for future research. Moreover, there is also a societal relevance for the thesis. The more research on cyber capacity building can

[12] Collett and Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios."

[13] Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities."

[14] Sadie Creese, William H. Dutton, and Patricia Esteve-González, "The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions," *Personal and Ubiquitous Computing*, 2021, https://doi.org/10.1007/s00779-021-01569-6.

[15] Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy"; Patryk Pawlak and Panagiota-Nayia Barmpaliou, "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity," *Journal of Cyber Policy* 2, no. 1 (2017): 123–44, https://doi.org/10.1080/23738871.2017.1294610; Alexander Klimburg and Hugo Zylberberg, "Cyber Security Capacity Building: Developing Access," no. 6 (2015); Johann Ole Willers, "Seeding the Cloud: Consultancy Services in the Nascent Field of Cyber Capacity Building," *Public Administration*, 2021, https://doi.org/10.1111/PADM.12773.

[16] Wolfgang Kleinwächter, "Framing the Internet Governance Debate: The Long Road to WSIS+20 (2025)," *CircleID*, March 4, 2021, https://circleid.com/posts/20210304-framing-the-internet-governance-debate-long-road-to-wsis-2025/.

increase to a better understanding of the concept and the incentives of stakeholders, which can lead to better global and regional coordination, and therefore a more efficient and effective use of the available resources.

1.3 Structure of thesis

The thesis is divided in the following chapters. The next chapter will provide a literature review and theoretical insights regarding the internet governance debate, the concept of (cyber) capacity building, and its link to foreign policy objectives by answering the sub-research question: what is Cyber Capacity Building and how is it linked to foreign policy objectives? In the third chapter, the research design will highlight and explain why this study has chosen a qualitative comparative case study through triangulation methods to collect data using open-source databases such as the UN voting records and Cybil – the CCB knowledge portal, semi-structured interviews, and desk research. The chapter will conclude with the analytical framework that will be used for the analysis part of the thesis. The fourth chapter presents the analysis in three parts and will answer the remaining three sub-research questions: i) What are the internet governance divisions in the international arena? ii) Which countries receive cyber capacity support from donor countries? and iii) What are the motivations of countries to invest in cyber capacity building activities? The final chapter of the thesis will focus on the conclusion and recommendations for future research.

2. Literature review and theoretical considerations

This section will cover the literature review and theoretical framework part of the thesis by focusing to answer the following sub-research question: What is Cyber Capacity Building and how is it linked to foreign policy objectives? The literature review will first focus on the internet governance debate to gain a better understanding of the issue and the geopolitical considerations. Secondly, the concept of Cyber Capacity Building will be examined more closely, specifically what the academic debate has identified as incentives for international cyber capacity building and what are the challenges. Thirdly, this section will focus on how capacity building in general can be linked to foreign policy objectives. The fourth and last part of the literature review will answer the sub-research question by presenting a theoretical framework and an explanation on how this thesis contributes to the ongoing academic debate.

2.1 Internet governance debate in an international context

This section will focus on examining the internet governance debate in an international context. Starting with the origins of the internet and the growing issue regarding its governance. The second sub-section will focus on the different perspectives on the governance of the internet and the geopolitical divisions. The last part in this section will explore how the internet governance debate fits within the international context and its latest developments that are relevant to the thesis.

2.1.1 Origins of the internet governance debate

To gain a better understanding of the debate on internet governance, it is important to understand what is meant with both 'governance' and the 'Internet'. In the 1970s, the notion arose that not just governments (state actors), but also non-state actors can have a role in the regulation of society besides governments on a local, regional, and global level.[17] Examples of non-state actors are private companies, non-governmental organizations (NGOs), lobby groups; in sum any stakeholder that is not affiliated with the government. In the past, the core responsibility of the state was to ensure protection and security for its citizens; in the 21st century, this same responsibility can be observed in the state providing social security, education, healthcare and infrastructure and many other services.[18] Nowadays, even though

[17] Scholte, "Polycentrism and Democracy in internet Governance," no. 165 (2017): 165–84.

[18] Peter Wijninga et al., "4 State and Non-State Actors: Beyond the Dichotomy," in *Strategic Monitor 2014: Four Strategic Challenges*, ed. Joris Van Esch et al., 2014, 141–62, https://www.jstor.org/stable/pdf/resrep12608.8.pdf?refreqid=excelsior%3A4a4f2bf59c47e305ab35931ed0c7ceb7.

non-state actors generally cannot control a population and a territory, they can still influence the governance of a country on particular issues. Therefore, governance can be best understood according to Stoker[19] and Rosenau[20] as an umbrella term of the different varieties of policy-making that includes the actions of the government as well as the actions from non-state actors.[21]

In the late 1960s, the internet started out as an American university project: ARPANET. Since its initial development, the internet has been governed by various institutions, processes, and actors. A wide range of actors was involved in the development and expansion of what is today known as the internet: academics, engineers, software developers, international organizations, telecommunications companies, and to a lesser extent governments also played a role.[22] The most important element to highlight here is that there was no singe actor who decided on the development of the internet or how it should be governed. At the time of the development of the internet, no one could have imagined the impact it would have on today's global society with in the 21st century having all economic and social structures running on the internet infrastructure. With the extreme growth and expansion of the internet, the issue of governance also arose along with the growing concerns about cybersecurity threats.

In the early 2000s, Kofi Annan, the Secretary-General of the UN, mandated a Working Group on Internet Governance (WGIG) as a response to concerns over the governance of the internet. Countries were specifically concerned over the role and control of the United States regarding the internet, since their Commerce Department contracted ICANN – the Internet Corporation for Assigned Names and Numbers) – the organization responsible for the administration of internet names and numbers on a global level.[23] The WGIG agreed on a working definition for Internet Governance: *"it is the development and application by Governments, the private sectors and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet"*.[24] The

[19] Gerry Stoker, "Governance as Theory: Five Propositions," *International Social Science Journal* 68, no. 227–228 (March 1, 2018): 15–24, https://doi.org/10.1111/ISSJ.12189.

[20] James N Rosenau, "Governance in the Twenty-First Century," *Source: Global Governance* 1, no. 1 (1995): 13–43.

[21] David Morar, "Perspectives on Internet Governance: (Why) Does Internet Governance Matter?," 2016.

[22] Lawrence E Strickling and Jonah Force Hill, "Multi-Stakeholder Internet Governance : Successes and Opportunities," *Journal of Cyber Policy* 2, no. 3 (2017): 296–317, https://doi.org/10.1080/23738871.2017.1404619.

[23] Laura Denardis and Mark Raymond, "Thinking Clearly about Multistakeholder Internet Governance," 2013.

[24] Château De Bossey, "Report of the Working Group on Internet Governance," 2005.

WGIG's definition designated a role for governments in internet governance corresponding to the increased interest of countries to have a more prominent role themselves or through intergovernmental entities, such as the UN.[25]

Since 2005, the academic debate on internet governance has significantly expanded to explain the concept of internet governance, and specifically on the role of states. Nye applied the concept of regime complex to the management of global cyber activities to demonstrate the different types of actors and activities that are involved in this process, wherein states are only one of the many actors.[26] DeNardis and Raymond attempt to understand the internet governance ecosystem according to its six main functions: 1) control of critical internet resources; 2) setting internet standards; 3) access and interconnection coordination; 4) cybersecurity governance; 5) policy role of information intermediaries; and 6) architecture-based intellectual property rights enforcement. Moreover, they argue that internet governance is not a singular endeavor, but that it involves many layers with distinct tasks wherein governments have either been uninvolved or their only involvement has been as participants lacking any decision-making authority.[27] Furthermore, Scholte considers internet governance from a polycentric perspective due to its characteristics by its *"trans-scalarity, trans-sectorality, diffusion, fluidity, overlapping mandates, ambiguous hierarchies and a post-sovereign absence of a single and consistent supreme authority*" and identifies six ways for democratic governance on the internet: 1) communitarianism; 2) multilateralism; 3) cosmopolitan federalism; 4) stakeholderism; 5) deliberation; and 6) counter-hegemonic resistance.[28] Most of the available literature focuses more on who can contribute to the discussions of internet governance, and there is a lack of studies on which actors can play a role in the actual practice of it.[29]

All in all, over the past decades, especially governments are increasingly claiming their role in the governance of the internet, and in this competition of the redistribution of power, they are not only competing with other actors, but mostly amongst each other due to different ideologies of the internet.

[25] Denardis and Raymond, "Thinking Clearly about Multistakeholder Internet Governance."

[26] Joseph S Nye, "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance*, vol. 1, 2014, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

[27] Denardis and Raymond, "Thinking Clearly about Multistakeholder Internet Governance."

[28] Scholte, "Polycentrism and Democracy in Internet Governance."

[29] Denardis and Raymond, "Thinking Clearly about Multistakeholder Internet Governance."

2.1.2 Internet ideologies and geopolitical divisions

Within the internet governance debate, the literature identifies two different types of ideologies that define and determine the behavior or position of states. The first ideology is described by most academics as the 'multi-stakeholder approach', the second ideology as a 'multilateral approach'. Although this debate has deep rotes, one of the key discussion points, as highlighted by Kurbalija[30] and many others, concerns the internet being 'open'. The openness of the internet is related to the technical side and refers to the absence of prohibitive restrictions on the internet, for example censorship or limited access.[31] The multi-stakeholder ideology strongly supports the notion of an open internet, and critique of an open internet by certain countries is considered a critique on the multi-stakeholder approach. Additionally, the multi-stakeholder approach includes besides open, three other elements as described by Strickling. First, a stakeholder-driven approach wherein diverse actors determine both processes and decisions. Secondly, transparency to underline that all actors and the public have access to the discussions. Thirdly, consensus-based outcomes that are taken because of compromise by a majority and/or a diversity of stakeholders.[32] Many authors argue that since its inception, the internet has been governed through a multi-stakeholder approach. One notable example is the establishment of ICANN as it demonstrated that a group of different actors could establish a consensus plan for the organization and the accountability mechanisms for such a key organization within the internet governance process.[33]

As explained above, states have traditionally been solely responsible for all issues regarding security. However, the internet governance debate, that covers security and other aspects, involves other stakeholders including civil society and the private sector. This creates a unique situation where governments need to share the ownership and responsibility of such an important domain with non-state actors.[34] However, there are several challenges with regarding the multi-stakeholder approach. For instance, the legitimacy problem: who determines which actors are relevant in internet governance, especially from the private sector and civil society,

[30] Jovan Kurbalija, *An Introduction to Internet Governance*, 7th ed. (Geneva: DiploFoundation), accessed October 28, 2021, https://wp4.diplomacy.edu/sites/default/files/AnIntroductiontoIG_7th edition.pdf.

[31] Morar, "Perspectives on Internet Governance: (Why) Does Internet Governance Matter?"

[32] Strickling and Hill, "Multi-Stakeholder Internet Governance : Successes and Opportunities."

[33] Strickling and Hill.

[34] Alexander Klimburg and Louk Faesen, "A Balance of Power in Cyberspace," in *Governing Cyberspace: Behavior, Power, and Diplomacy*, ed. Dennis Broeders and Bibi Van den Berg (London: Rowman & Littlefield, 2020), 145–71, https://www.researchgate.net/profile/Dennis-Broeders-2/publication/343833386_Governing_Cyberspace_Behavior_Power_and_Diplomacy/links/5f43c484a6fdcccc43f584f0/Governing-Cyberspace-Behavior-Power-and-Diplomacy.pdf#page=154.

and how do they gain the authority on outcomes in the process?[35] A second challenge is consensus, similarly to the legitimacy problem, it is unclear when consensus is reached in a multi-stakeholder approach, since unanimity is impossible to reach, and which actors get a vote and what is the weight of their vote?[36]

The above arguments are examples used by the opposing ideology within the internet governance debate, the multilateral approach. Proponents of this approach strive for more self-preservation of countries and international organizations' roles as regulators and argue that the internet should be regulated under existing global bodies. Such an approach would also mean an enormous increase in the role for countries in the regulation of the internet. These countries endeavor to give the UN more control over the internet, since only countries are represented at the UN.[37] Therefore, opponents of the multilateral approach fear the implications that a more controlled internet could have regarding fundamental principles, such as civil liberties and censorship that are linked to a government's approach towards democracy.[38]

The international arena is divided along these two ideologies. DeNardis and Raymond explain this as the Organization for Economic Co-operation and Development (OECD) versus the Shanghai Cooperation Organization (SCO) views. The OECD view, which is held by most of the Member States of the OECD, is in line with the multi-stakeholder approach that commits to the rule of law. The SCO view, which is primarily held by China, Russia, and other members of the SCO, underscores a strong and conditional understanding of sovereignty with regard to internet governance, and it views a hierarchical state-society relationship with limited input from other non-state actors.[39] This geopolitical divide became evident in 2012, when 54 countries refused to sign the revised International Telecommunication Regulations (ITR) that attempted to increase the role of the International Telecommunication Union (ITU) that would promote a more prominent role for states and therefore the multilateral approach.[40] The criticism of this revised document by the United States and 53 other states as well as non-state actors was focused on the potential harm it could cause to the open character of the internet.

[35] Klimburg and Faesen.

[36] Strickling and Hill, "Multi-Stakeholder Internet Governance : Successes and Opportunities."

[37] Alix Desforges, "Representations of the Cyberspace: A Geopolitical Tool," *Herodote*, no. 152–153 (2014): 67–81, https://doi.org/10.3917/her.152.0067.

[38] Morar, "Perspectives on Internet Governance: (Why) Does Internet Governance Matter?"

[39] Denardis and Raymond, "Thinking Clearly about Multistakeholder Internet Governance."

[40] Desforges, "Representations of the Cyberspace: A Geopolitical Tool"; Morar, "Perspectives on Internet Governance: (Why) Does Internet Governance Matter?"

The internet governance debate has been ongoing ever since on different fora, including the UN First and Third Committees.

In sum, Broeders and Van den Berg highlight this divide between the multi-stakeholder and multilateral approaches exacerbates the geopolitical tension between global powers through interstate behavior, such as cyber operations, as well the positions of states in the diplomatic negotiations on an international level regarding 'responsible state behavior in cyberspace'.[41] Since these diplomatic negotiations are essential for the analysis in the thesis, the UN cybersecurity processes are elaborated further below.

2.1.3 The international arena of the internet governance debate

Over the past decades, the UN has been the central arena for states to engage with each other on the internet governance debate. In 2004, a venue was created at the UN level to discuss the developments in the field of Information and Telecommunications in the context of International Security: the UN Group of Governmental Experts (UN GGE). Four out of the six iterations of the UN GGE resulted in a consensus report, in 2013 yielding that international law can be applied in cyberspace, and in 2015 with the construction of 11 nonbinding norms regarding responsible state behavior in cyberspace.[42] Another important element of the 2015 GGE consensus report was the mentioning of the importance of cyber capacity building: *"While [normative] measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity"*.[43] The 2017 UN GGE failed, but in November 2018, the UN General Assembly (UNGA) voted on two parallel and competing resolutions, that both got accepted. Interestingly both resolutions got accepted by the UN General Assembly, and both the UN GGE and OEWG started in 2019.

- **A/RES/73/27**[44] – this 2018 resolution was submitted by Russia and called for an Open-Ended Working Group to discuss the development of rules, norms and principles of responsible state behavior of states and their implementation, as well as to explore the

[41] Dennis Broeders and Bibi van den Berg, "Governing Cyberspace Behavior, Power, and Diplomacy," ed. Dennis Broeders and Bibi van den Berg (Rowman & Littlefield, 2020).
[42] Broeders and Berg.
[43] United Nations General Assembly, "United Nations General Assembly Consensus Report GGE 2015: A/70/174," 2015, https://undocs.org/A/70/174.
[44] United Nations General Assembly, "UNGA Resolution A/RES/73/27: Developments in the Field of Information and Telecommunications in the Context of International Security" (UN, December 11, 2018), https://digitallibrary.un.org/record/1655670.

possibility of the establishment of regular formal dialogue with wide-ranging participation at the UN.[45] Furter, all interested UN Member States were invited to join this process and additionally it would organize consultation meetings with interested non-state actors.

- **A/RES/73/266**[46] – this 2018 resolution was submitted by the United States to establish a new UN GGE on Advancing responsible state behavior in cyberspace in the context of international security. Besides the five permanent members of the UN Security Council, the other remaining seats are allocated by regional grouping through an expression of interest.[47]

There have been three other Russian sponsored UNGA resolutions that have required voting over the past years:

- **A/RES/73/187**[48] – this 2018 Russian sponsored resolution in the Third Committee of the UN General Assembly on countering the use of information and communication technologies for criminal purposes that could launch a process to result in and international treaty on cybercrime.[49]
- **A/RES/74/247**[50] – the 2019 Russian sponsored resolution again in the Third Committee called for the establishment of an Open-Ended Cybercrime Ad Hoc Committee.
- **A/RES/75/240**[51] – this 2020 Russian sponsored resolution called in the First Committee for a renewal of the OEWG that was established in 2018 and was renewed for the period of 2021-2025.

[45] Digital Watch Observatory, "UN GGE and OEWG," accessed February 26, 2021, https://dig.watch/processes/un-gge.
[46] United Nations General Assembly, "UNGA Resolution A/RES/73/266: Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (UN, January 2, 2019), https://digitallibrary.un.org/record/1658328.
[47] Digital Watch Observatory, "UN GGE and OEWG."
[48] United Nations General Assembly, "UNGA Resolution A/RES/73/187: Countering the Use of Information and Communications Technologies for Criminal Purposes" (UN, January 14, 2019), https://digitallibrary.un.org/record/1660536.
[49] Justin Sherman and Robert Morgus, "Breaking Down the Vote on Russia's New Cybercrime Resolution at the UN," *New America*, 2018, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/breaking-down-vote-russias-new-cybercrime-resolution-un/.
[50] United Nations General Assembly, "UNGA Resolution A/RES/74/247: Countering the Use of Information and Communications Technologies for Criminal Purposes" (UN, January 20, 2020), https://digitallibrary.un.org/record/3847855.
[51] United Nations General Assembly, "UNGA Resolution A/RES/75/240: Developments in the Field of Information and Telecommunications in the Context of International Security" (UN, January 4, 2021), https://digitallibrary.un.org/record/3896458.

These five UNGA resolutions demonstrate that it is the United States and the Russians who have sponsored resolutions in the UN First and Third Committees over the past years to steer the conversation that will impact the internet governance debate. These UNGA resolutions will be relevant for the analysis of the thesis.

The previous sub-section highlighted the two sides of the internet governance debate, and therefore it is not surprising that Russia votes against US sponsored regulations and vice versa. There is also a third group in the international arena that gets overlooked by some academics. This group is what Morgus refers to as the 'digital deciders' or the 'digital swing states', the countries that mostly remain undecided on which ideology to align with, and therefore possess the capability to influence the global conversation. This group is quite large, with over 100 countries including developing countries and LDCs, and can become the key factor in determining the future of the internet and its governance by taking on new responsibilities, obscuring solutions with more challenges, or by free riding on established countries' positions if they find alignment with either ideology.[52]

Furthermore, since the mentioning of cyber capacity building in the 2015 GGE consensus report, the topic has been included and increased in its importance in the other GGE and OEWG conversations. as well as a priority for countries to increase their cyber capacities. Homburger argues that through these UN processes, cyber capacity building is presented as the vital tool to both implement the agreed upon cyber norms as well as to increase the ICT development and cyber maturity of developing countries.[53] Cyber capacity building was mentioned in the thesis introduction as a tool to achieve foreign policy objectives by countries, but it is also important to highlight that it presented as a key priority for countries to increase their own capacity and to help others to increase their cyber capacity in the ongoing dialogues at the UN level.

In sum, the internet governance debate is a complex issue with two main opposing ideologies that causes geopolitical divisions in the international arena. For the remainder of the thesis, these two groups will be referred to as the "multi-stakeholder and open" group and the

[52] Robert Morgus, Jocelyn Woolbright, and Justin Sherman, "The Digital Deciders," 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

[53] Zine Homburger, "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace," *Https://Doi.Org/10.1080/13600826.2019.1569502* 33, no. 2 (April 3, 2019): 224–42, https://doi.org/10.1080/13600826.2019.1569502; Robert Collett, "Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures," *Journal of Cyber Policy*, 2021, https://doi.org/10.1080/23738871.2021.1948582.

"sovereign and controlled" group. One key to success for both sides of the debate lies in convincing the digital swing states to align with their position, which could steer the international dialogue at the UN level in their direction. The next section will explore how cyber capacity building can be used as a tool to for foreign policy objectives as well as its other drivers.

2.2 Cyber capacity building: development aid, incentives, and obstacles

In the second section of the literature review, the concept of cyber capacity building will be examined more closely, specifically what the academic debate has identified as incentives for cyber capacity building and what the challenges are. As cyber capacity building is a form of capacity building, this section will start with capacity building activities in general.

2.2.1 Capacity building as an approach of development aid

Capacity building is a form of development aid, which has a common objective to alleviate poverty and to improve the livelihood of the local population.[54] These different forms of development aid have evolved since the 1950s from technical supply-driven assistance towards a more demand-driven approach focused on outcomes.[55] Therefore, capacity building was the successor in the late 1990s of other development aid concepts as Institutional Building, Institutional Strengthening, Human Resource Development and New Institutionalism after a discussion regarding the effectiveness of development aid programs.[56]

The general agreement amongst academics and organizations is that capacity building presumes that the local government and stakeholders are most suitable to identify and address their own challenges and that development programs should therefore aim to assist the local actors, rather than replace them, which will lead to more sustainable, effective and efficient outcomes.[57] The

[54] Bertha Vallejo and Uta Wehn, "Capacity Development Evaluation: The Challenge of the Results Agenda and Measuring Return on Investment in the Global South," *World Development* 79 (2016): 1–13, https://doi.org/10.1016/j.worlddev.2015.10.044.

[55] UNDP Capacity Development Group, "Overview of UNDP's Approach to Supporting Capacity Development," no. August (2009); Vallejo and Wehn, "Capacity Development Evaluation: The Challenge of the Results Agenda and Measuring Return on Investment in the Global South."

[56] Stefan Kühl, "Capacity Development as the Model for Development Aid Organizations," *Development and Change* 40, no. 3 (2009): 551–77, https://doi.org/10.1111/j.1467-7660.2009.01538.x.

[57] Kevin P. Clements et al., "State Building Reconsidered: The Role of Hybridity in the Formation of Political Order," *Http://Dx.Doi.Org/10.1177/003231870705900106* 59, no. 1 (2017): 45–56, https://doi.org/10.1177/003231870705900106; Timothy Edmunds and Ana Juncos, "Constructing the Capable State: Contested Discourses and Practices in EU Capacity Building," *Cooperation and Conflict* 55, no. 1 (2020): 3–21.

United Nations Development Programme (UNDP) has defined capacity building as "the process by which individuals, groups, organizations, institutions and societies increase their abilities to: (i) perform core functions, solve problems, define and achieve objectives; and (ii) understand and deal with their development needs in a broad context and in a sustainable manner".[58] Moreover, capacity building can be seen as an umbrella concept encompassing the other previous approaches of development aid as it seeks social change through sustainable economic and social development from a demand-driven and long-term perspective.[59]

However, the above view on capacity building is questioned by various academics who argue that the 'capacity' support being provided can disguise the preference for a specific set of social and political approaches[60] and therefore argue that the Western ideas and its agenda should not dominate the capacity building activities targeted at recipients[61]. This has led to the assumption that capacity building activities can be used as a foreign policy tool to further national interests on an ideological, security, and economical level.[62] Moreover, with regard to capacity building activities in the context of cybersecurity, that through continuous activities such as sharing of best practices and the identification of needs, that this will eventually result not only in a higher level of cyber resilience, but also in an "alignment of positions" between donors and recipients.[63]

2.2.2 Cyber Capacity Building

Compared to other fields of international collaboration, the field of cyber capacity building is still young with its origin in the late 1990s and becoming more commonly used during the last twenty years.[64] Pawlak used the term in 2014 as to describe it as an *"umbrella concept for all types of activities that safeguard and promote the sage, secure, and open use of cyberspace"*.[65]

[58] United Nations Development Programma (UNDP), "Capacity Development: A UNDP Primer," 2009.

[59] Vallejo and Wehn, "Capacity Development Evaluation: The Challenge of the Results Agenda and Measuring Return on Investment in the Global South."

[60] Shahar Hameiri, "Capacity and Its Fallacies: International State Building as State Transformation," *Millennium: Journal of International Studies* 38, no. 1 (2009): 55–81, https://doi.org/10.1177/0305829809335942.

[61] Mary Kaldor, Mary Martin, and Sabine Selchow, "Human Security: A New Strategic Narrative for Europe," *International Affairs* 83, no. 2 (2007): 273–88, https://doi.org/10.1111/j.1468-2346.2007.00618.x.

[62] David Chandler, *International Statebuilding: The Rise of Post-Liberal Governance* (London: Routledge, 2010); Timothy Donais, "Inclusion or Exclusion? Local Ownership and Security Sector Reform," *Studies in Social Justice* 3, no. 1 (2009): 117–31, https://doi.org/10.26522/ssj.v3i1.1027; Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy."

[63] Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy."

[64] Collett and Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios."

[65] Patryk Pawlak, "Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development," *Issue* 21, no. December (2014), https://doi.org/10.2815/43313.

Similar to many other concepts in the field of cybersecurity, the concept of cyber capacity building lacks a commonly agreed upon definition. The aim of cyber capacity building is well described by Dutton et al, as the development of *"a supportive environment for enabling cybersecurity"*.[66] However, for the purpose of this thesis, the definition by Calderaro and Craig is used as it demonstrates which topics cyber capacity building encompasses: *"cyber capacity is about achieving resilience against internet-based threats through a range of policies which include the creation of national cybersecurity strategies, computer security incident response teams (CSIRT), the strengthening of cybercrime laws, the promotion of public-private partnerships, and improved education and awareness*".[67]

Although there are different types of cyber capacity building activities and between different stakeholders,[68] as the above definition indicates and when the concept is used in the academic debate, it refers almost always distinctly to a donor-recipient relationship through development aid.[69] There are multiple arguments why countries engage in cyber capacity building activities.

For instance, Klimburg and Zylberberg identify cyber capacity building incentives through a three-fold approach: first of all, the sustainable development incentive to establish a foundation to benefit from the political, economic, and social dividends that the internet offers; secondly, the security incentive to bridge the digital divide that developing countries are able to respond to cybersecurity threats; and thirdly, the foreign policy incentive as it is an opportunity to promote a favored model of internet governance since many developing countries have a 'swing-state position' in the international debate."[70] This is in line with the different incentives that Pawlak and Barmpaliou have observed in the academic debate, they frame it as "economic and social development, cyber resilience, and the pursuit of foreign policy objectives".[71] Therefore, the next section will dive deeper into these three various incentives by drawing on

[66] William H Dutton et al., "Cybersecurity Capacity," *Journal of Information Policy* 9, no. May 2021 (2019): 280–306.

[67] Calderaro and Craig, "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building."

[68] As described by Robert Collett (2021, p. 7), there are different types of cyber capacity building: 1) between North-South; 2) between North-South-South; 3) Triangular; and 4) Multidirectional.

[69] Hohmann et al., "Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach"; Niels Nagelhus Schia, "The Cyber Frontier and Digital Pitfalls in the Global South," *Third World Quarterly* 39, no. 5 (2018): 821–37, https://doi.org/10.1080/01436597.2017.1408403; Willers, "Seeding the Cloud: Consultancy Services in the Nascent Field of Cyber Capacity Building"; Collett, "Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures."

[70] Klimburg and Zylberberg, "Cyber Security Capacity Building: Developing Access."

[71] Pawlak and Barmpaliou, "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity."

literature of other actors, grouping them as: development, security, and the foreign policy incentives.

2.2.3 Development, security, and foreign policy incentives for cyber capacity building

First, the reasoning behind the development incentive fits with the importance and necessity for global digital development in all countries. It has become clearly evident that digitalization has become a crucial component for social, political, and economic development. Additionally, digitalization has spill-over effects to other sectors and other parts of society, for example education, energy, and health.[72] Yet, there is a still a large digital divide both within countries, for example between rural and city areas, as well as between countries.[73] For example, from the developed countries 72.12% had access to the internet in 2010 that increased to 82.43% in 2017. In comparison, only 4% of the LDCs were connected to the internet in 2010 and that percentage increased to 17.78% in 2017.[74] Therefore, bridging the digital divide is a priority on the international level as is demonstrated through one of the United Nation's Sustainable Development Goals (SDGs), under SDG number 9, the aim is "*to significantly increase access to ICT and strive to provide universal and affordable access to the internet in least developed countries*".[75]

The high and broad impact of digitalization for developing countries also has an impact on how donor countries and organizations can support sustainable development and contribute to achieving the SDGs. There is broad consensus on the importance of connecting developing countries to digital networks, to avoid widening the gap between rich and poor states.[76] Additionally, as presented in a recent paper by Schia and Willers, the impact of cyber capacity building goes even beyond just the benefit of SDG 9, but also supports the other SDGs. For instance, digitalization and internet access can enable societies to have better working conditions and an increased income (SDG 8), digital solutions can provide better access to health services (SDG 3), improve opportunities for a better education (SDG 4), and through

[72] Hohmann et al., "Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach."
[73] The World Bank Group, *Digital Dividends*.
[74] Calderaro and Craig, "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building."
[75] United Nations, "Transforming Our World: The 2030 Agenda for Sustainable Development."
[76] "Principles | Principles for Digital Development," accessed October 3, 2021, https://digitalprinciples.org/principles/.

increased cooperation and partnership can even be a contributing factor to ending poverty and hunger (SDG 1 and 2).[77]

Therefore, there is broad support recognition on the need to support developing countries with their digital efforts in order for them to reap the digital dividends that the internet offers. Over the past few decades, significant success has already been made. In 2003, only 10% of the world's population had access to the internet, mostly in North America and Western Europe; whilst today almost 50% of the world's population is connected to the internet – this large increase is especially the result of the Global South's increased access and connectivity.[78]

Although this is a great achievement, it does bring new challenges, especially regarding security as highlighted by Schia, who notes that the ICT infrastructure hosted by developing countries is often used by actors conducting malicious cyber activities.[79]

Therefore, the second incentive – security - is an important motivator for countries to engage in cyber capacity building activities, especially since such malicious cyber activities are a potential threat to donor countries. The argument from Klimburg and Zylberberg is linked to the need to raise the cyber resilience level of developing countries to be better prepared against cyber threats. Due to the significant growth of digitalization, especially in developing countries, this also results in rapid growth of cyber threats, for example data breaches, cybercrime, and attacks on critical infrastructure. Hohmahn et al. observe that the challenge with the fast speed that developing countries are gaining access to the internet can lead to the fact that cybersecurity becomes an afterthought.[80]

This is a concern for all countries since cyberspace crosses borders and allows any actor to attack another actor anywhere around the world. Therefore, this is another key incentive for donor countries to engage in international cyber capacity building activities to fight against cybercrime and cyber threats. There are challenges due to the security and development nexus, also called the security vs access debate.[81] In theory, it seems simple that access and security

[77] Niels Nagelhus Schia and Johann Ole Willers, "Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries," no. February (2021): 221–30, https://doi.org/10.1007/978-3-319-95873-6_115.

[78] Calderaro and Craig, "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building."

[79] Schia, "The Cyber Frontier and Digital Pitfalls in the Global South."

[80] Hohmann et al., "Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach."

[81] Klimburg and Zylberberg, "Cyber Security Capacity Building: Developing Access."

should go hand-in-hand, nevertheless in practice it is much more complex to balance internet access and cybersecurity programs. A number of reasons for this are because they are separate efforts, implemented by distinct stakeholders, linked through different strategies and budgets.[82] Nonetheless, as actors such as Internet Society (ISOC) highlight, the consequence of the security vs access debate is diminishing trust, which can be identified as *"poor cybersecurity"* that will limit the use and effectiveness of the internet and limit the implementation of the SDGs.[83] Therefore, there is a challenge to create a stable and institutional structure for countries to utilize the internet, whilst having the capabilities to properly protect their infrastructure and citizens from threats.[84]

In sum, the security incentive for donor countries refers to strengthening the capabilities of developing countries to increase their level of cyber resilience that will indirectly benefit their own national security as well. There are also direct benefits for the donor countries and their own security interests. Cyber capacity building can lead to the intensifying collaboration between the intelligence and military services of both countries.[85]

Thirdly, the foreign policy incentive is linked to the notion that cyber capacity building is used as a tool for donor countries to further their own national interests, either political or ideological, for example regarding the position of a country in the internet governance debate. Section 2.1 of the literature review underlined that there are different ideologies regarding the governing of the internet that are linked to many other geopolitical issues and considerations in the international arena. Therefore, it is not surprising that cyber capacity building is observed as a tool for donor countries to further their own national interests.

Hohmann et al highlight that cyber capacity building can be helpful when advocating for a particular model of internet governance, but also to create access to the recipient's market for their domestic companies, and to promote preferred internet standards.[86] Klimburg & Zylberberg argue one step further by stating that cyber capabilities cannot be developed in a

[82] Jonathan Dolan, "Digital Inclusion and a Trusted Internet: The Role of the International Development Community in Balancing Internet Access and Cybersecurity," *DAI*, no. October (2018).
[83] Internet Society (ISOC), "A Policy Framework for an Open and Trusted Internet: An Approach for Reinforcing Trust in an Open Environment," 2017; Robert Morgus, "Securing Digital Dividends Mainstreaming Cybersecurity in International Development," 2018.
[84] Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities."
[85] Klimburg and Zylberberg, "Cyber Security Capacity Building: Developing Access."
[86] Hohmann et al., "Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach."

vacuum; these capacities are influenced by various ideological and political interests, since through engagement with all relevant local actors, cyber capacity activities form a unique opportunity for donors to use their soft power to spread the norms of like-minded countries.[87] Additionally, Pawlak notes that donor countries increasingly consider cyber capacity building projects as an opportunity to promote their preferred vision of cyberspace whilst addressing the needs and supporting the cyber capacity needs of the recipient countries.[88] ‘

Furthermore, Pawlak has written an article in 2016 on the use of cyber capacity building as an instrument for foreign policy. He explored the linkages between the international debates on cyber-related issues and cyber capacity building with a specific focus on the activities of the Council of Europe and ITU. He identifies four different global cyber-related debates: cybercrime, privacy, international stability, and internet governance. He concludes that cyber capacity building is tailored to further foreign policy objectives, but that process of ideological alignment between donors and recipients requires further analysis.[89]

This thesis will apply these three identified incentives for donor countries to engage in cyber capacity building to the remainder of this study. It should be highlighted that donor countries can often have multiple or a combination of the three incentives: development, security, and foreign policy objectives.

2.2.4 Obstacles to cyber capacity building investments

For the purpose of this thesis, it is also relevant to gain a better understanding of the obstacles to cyber security building investments that donors face. There are five main obstacles mentioned by multiple authors in the academic debate, and these are elaborated on below.

The first obstacle is linked to the obtainment of correct and relevant information regarding the level of cyber capacity in a potential recipient country. This information is essential in determining the support that is required by a donor, nonetheless countries do not always want to share this data, or they are not aware of their capacities and/or capacity needs, which makes it difficult for countries to pursue a demand-driven approach.[90] A secondly obstacle related is

[87] Klimburg and Zylberberg, “Cyber Security Capacity Building: Developing Access.”
[88] Pawlak, “Capacity Building in Cyberspace as an Instrument of Foreign Policy.”
[89] Pawlak.
[90] Muller, “Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities.”

that there is a thin line between encouraging countries to develop certain cyber capacities as well as to avoid imposing Western ideas and concepts that donors need to balance carefully.[91] The third obstacle is related to official development assistance (ODA) funding, the rules and criteria for development aid set out by OECD to "promote and target the economic development and welfare of developing countries" and exclude "military aid and promotion of donors' security interests".[92] There are two problems linked to the ODA funding obstacle: 1) the limitations to ODA funding can exclude some donor countries for using their ODA funding for cyber capacity building activities;[93] and 2) not all developing countries have the ODA status and therefore there is an imbalance between some countries who receive high amounts of ODA compared to countries who receive funding disproportionate to their needs.[94] A fourth obstacle is the lack of coordination between donors on cyber capacity efforts that is worsened by the growing gap between aspirations and the implementation of cyber capacity building activities.[95] The fifth and last obstacle that donors face is linked to the dilemma how these donors can ensure that the expertise shared with recipients will not be used against themselves? For instance, with technical training cyber capacity activities, donors share expertise on how to develop a CSIRT for a country to protect itself against cybersecurity attacks, knowledge is also provided on cybersecurity attacks.[96]

In sum, the above incentives and obstacles to cyber capacity building that are identified in the academic debate are relevant for the analysis to have a better understanding on the drivers for international cyber capacity building investments by donor countries. The next section will link cyber capacity building to foreign policy objectives.

2.3 Linking cyber capacity building to foreign policy objectives

In order to examine how cyber capacity building can be used as a tool to further a country's foreign policy objectives, this section will situate the concept of cyber capacity building in a broader theoretical context regarding a state's foreign policy instruments. First, looking at how

[91] Klimburg and Zylberberg, "Cyber Security Capacity Building: Developing Access"; Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities."

[92] OECD, "Official Development Assistance (ODA) What Is ODA?," 2019, www.oecd.org/dac.

[93] Melissa Hathaway and Francesca Spidalieri, "Integrating Cyber Capacity into the Digital Development Agenda," 2021, www.digitaldevelopmentpartnership.org.

[94] Pawlak and Barmpaliou, "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity."

[95] Collett and Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios."

[96] Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities."

foreign policy is linked to hard and soft power, then focusing on how development aid is used as a tool for foreign policy, since cyber capacity building is a form of this.

2.3.1 Foreign policy and power

Within the international context, all countries are in one way or another dependent on other countries in order to safeguard and further their own interests. Since cooperation with other countries is therefore a necessity, all countries have their foreign policy objectives to consider.[97] Every country establishes and maintains political, diplomatic, economic, trade, educational and cultural relationships with other countries and with international, and regional organizations, and with non-governmental actors. Therefore, the formulation of foreign policy can be defined as a country aiming "*to safeguard and promote its national interests in the conduct of relations with other countries, bilaterally and multilaterally… it is a direct reflection of a country's traditional values and overall national policies, her aspirations and self-perception*".[98]

Moreover, foreign policy is used by countries to achieve their national interests in the international arena. This is accomplished through foreign policy instruments, which is also referred to as 'instruments of power'. Power refers to the capability of an actor to influence the actions and behavior of others.[99] The notion is that power is conferred through the control of resources that are needed or valued by others, causing them to become dependent on the influencing actor to reach their own goals. In the academic debate, there are two main categories of power: hard power and soft power.

Hard power is the traditional form of foreign policy, which can be described as the ability to use military or economic coercion to have others follow your will.[100] More relevant for this thesis, is the use of soft power. Soft power is coined by Nye as "*the ability to affect others through the co-optive means of framing the agenda, persuading, and eliciting positive attraction in order to obtain preferred outcomes*".[101] Soft power is based on the idea to shape the preferences and ideas of others through attraction, however political results are not

[97] Jesmine Ahmed, "The Theoretical Significance of Foreign Policy in International Relatons: An Analysis" 7, no. 2 (2020): 787–92.

[98] Ahmed.

[99] Robert A Dahl, "The Concept of Power," *Behavioral Science* 2, no. 3 (1957), https://fbaum.unc.edu/teaching/articles/Dahl_Power_1957.pdf.

[100] Joseph Jr Nye, *Soft Power: The Means to Success in World Politics* (New York Public Affairs, 2004).

[101] Joseph Nye, "The Future of Power" (London, May 10, 2011), https://www.chathamhouse.org/sites/default/files/public/Meetings/Meeting Transcripts/100511nye.pdf.

guaranteed.[102] Although, there are critics that are skeptical of the effectiveness of the use of soft power as a foreign policy tool compared to hard power,[103] the use of development aid and capacity building efforts as a potential tool for foreign policy can be understood through the lens of soft power promotion.

2.3.2 Diplomacy as a tool for foreign policy and development aid

The study of the politics of development aid has been a contested issue since the 1960s. According to Morgenthau, there are six types of development aid: 1) humanitarian foreign aid, 2) subsistence foreign aid, 3) military foreign aid, 4) bribery, 5) prestige foreign aid, and 6) foreign aid for economic development. Morgenthau states that besides humanitarian aid, all the other types of aid are always political, and therefore can be considered a part of foreign policy objectives.[104]

Further, development aid shares several similarities with soft power promotion:

- It supports the creation of a positive image of the donor country, including gratitude;
- The donor country gets to transfer and share knowledge that includes the beliefs and values of the donor;
- Recipients are taking interest in the donor country and are incentivized to listen; and,
- Development aid is often based on immaterial resources as expertise on a diverse arsenal of topics[105], for instance cyber capacity building.

Therefore, it is not surprising that since development aid is closely linked to soft power, that there is a clear link between diplomacy as the instrument of soft power and development aid.

According to Ociepka, diplomacy can be understood as a two-way form of political dialogue targeted at foreign audiences with the aim to shape and enhance a positive image of the respective country.[106] There are numerous types of diplomacy, one of them is development

[102] Joseph Jr. Nye, *Soft Power: The Means To Success In World Politics*, *Helvetica Chimica Acta* (PublicAffairs, 2005).

[103] Niall Ferguson, *Colossus: The Price of America's Empire* (New York: Penguin Press, 2004); Collin S. Gray, "Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century," 2011.

[104] Hans Morgenthau, "The Political Theory of Foreign Aid Related Papers," 1965.

[105] Karolina Zielinska, "Development Diplomacy. Development Aid as a Part of Public Diplomacy in the Pursuit of Foreign Policy Aims: Theoretical and Practical Considerations," *Historia i Polityka* 16, no. 16 (2016): 9–26.

[106] Beata Ociepka, "Dyplomacja Publiczna," *Wydawnictwo Uniwersytetu Wrocławskiego*, 2008; Zielinska, "Development Diplomacy. Development Aid as a Part of Public Diplomacy in the Pursuit of Foreign Policy Aims: Theoretical and Practical Considerations."

diplomacy. Development diplomacy, also referred to 'sustainable development diplomacy' or 'global diplomacy', is aimed at the "*process of building a positive image abroad, bilateral relations and international role and position on the basis of aid transfers at promoting development and wellbeing of developing countries*".[107] There is a clear link between development diplomacy as a tool for foreign policy, according to Zielinska, when aid is provided in a manner that enhances a mutual, positive, and symmetric relationship, the more the recipient will be favorable to augment to the donor's soft power approach and thereby to alignment of positions.[108]

Nonetheless, there are two caveats that require further explanation. First of all, development diplomacy should be supported with other instruments of diplomacy, for instance social diplomacy, implying the assistance and involvement of NGOs, or educational diplomacy referring to the exchange of students and professionals to assist with the spreading of knowledge.[109] Secondly, it is essential to underline that development diplomacy should be intertwined within a broader strategy in the bilateral relationship between the donor and respective beneficiary, tailored to their national needs and political, economic and cultural environment.[110]

In sum, the above supports the statement made earlier in the literature review, that capacity building can be seen as an umbrella concept encompasses other approaches of development aid as it seeks social change through sustainable economic and social development from a demand-driven and long-term perspective.[111] Therefore, (cyber) capacity building can be seen as one of the soft power instruments that countries have available in their diplomatic toolbox to further their foreign objectives.

[107] Zielinska, "Development Diplomacy. Development Aid as a Part of Public Diplomacy in the Pursuit of Foreign Policy Aims: Theoretical and Practical Considerations."

[108] Zielinska.

[109] Nancy Snow, *Routledge Handbook of Public Diplomacy* , 2020, https://doi.org/10.4324/9780429465543.

[110] Zielinska, "Development Diplomacy. Development Aid as a Part of Public Diplomacy in the Pursuit of Foreign Policy Aims: Theoretical and Practical Considerations."

[111] Vallejo and Wehn, "Capacity Development Evaluation: The Challenge of the Results Agenda and Measuring Return on Investment in the Global South."

2.4 Theoretical framework for this thesis and the added value to the academic debate

The fourth and last part of the literature review will answer the sub-research question and will present a theoretical framework as well as an explanation on how this thesis contributes to the ongoing academic debate.

2.4.1 Theoretical framework of Thesis

The theoretical framework in Table 1 will be considered in the analysis of the thesis based on the above literature review. The literature review aimed to provide theoretical insights on the internet governance debate and explore the concept of cyber capacity building to illustrate how this can be linked to foreign policy objectives.

Table 1: Theoretical framework Thesis – Linking CCB to foreign policy objectives

Type of CCB	**Incentive**	**Impact**	**Tool for foreign policy**
Country to country (donor-recipient relationship)	**Development** • Economic • Social	→ Access to the internet and digital services accessible to local society	Soft power tools: Diplomacy Successful tool for foreign policy if: • Linked to other forms of diplomacy: social diplomacy, education diplomacy • Broader strategy of bilateral relationship between donor and recipient • Development aid needs to be tailored to national needs and environment
	Security	→ Capacities to increase cyber resilience against cyber threats	
	Foreign policy objectives	→ Alignment of ideologies on e.g., internet governance through e.g., participation in regional and international dialogues on cyber-related issues	
Obstacles to CCB investments • Difficulties to demand-driven approach • Balance between expertise and Western ideas • Linking cyber capacity building to ODA funding • Lack of coordination between donors • Technical training dilemma			

It was argued that cyber capacity building is a form of development aid that aims to develop a supportive environment to enable cybersecurity as stated by Dutton et al. In line with most of the available academic literature as well as for the purposes of this thesis, international cyber capacity building is considered as development aid assistance between a donor country and a recipient country. Various incentives for cyber capacity building were identified in the literature: development, security, and foreign policy incentives. As mentioned by Hameiri, Chandler and Pawlak, cyber capacity building can be used to promote foreign policy objectives on an ideological, security and economic level. For instance, the position of countries in the internet governance debate.

Furthermore, based on the above literature review, the hypothesis of this thesis is: *International cyber capacity building investments are targeted at like-minded countries and digital swing states*. This indicates that the position of a country in the internet governance debate can be used to guide a country's cyber capacity building investment, especially towards countries that consider the internet in a similar manner or are undecided. Chapter 3.7 will further explain how this hypothesis will be tested through the analytical framework in the analysis.

2.4.2 Added value of thesis to the academic debate

In the conclusion of Pawlak's article on the use of cyber capacity building as an instrument for foreign policy, he notes that this field is still *"under-researched"*.[112] This also becomes evident in the literature review presented. Although many articles refer to cyber capacity building being used for the pursuit of countries' foreign policy objectives, more in-depth research, as well as empirical evidence, is severely lacking.

Therefore, this thesis will contribute to the academic debate by interviewing various like-minded countries to gain a better understanding of their motivations in cyber capacity building investments and to what extent these are related to the internet governance debate as an example of furthering foreign policy objectives. In the analysis, this study will pioneer by using both open-source data on voting behavior to see where countries stand and combine this with cyber capacity building project data to explore which countries are targeted and whether this is linked to their position in the internet governance debate. Additionally, through interviews with donor countries the motivations behind cyber capacity building investments will be further explored. The current academic literature does not include empirical evidence collected through interviews from donor countries, therefore this thesis can provide new empirical evidence and knowledge to fill the knowledge gap in the academic debate.

[112] Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy."

3. Research Design

This chapter will explain the research design of the thesis. Starting with the research methodology, followed by the data sources, methods of data collection and justification and the ethics thereof. Moreover, the limitations and delimitations of the research design choices are explained followed by the case selection, and lastly the analytical framework for the analysis section will be presented. Recommendations on improving the research method in the future or other factors that could be considered will be reviewed in the Conclusion & Discussion of the thesis.

3.1 Research methodology

This thesis will follow a qualitative research methodology through a comparative case study method. A qualitative case study method allows the use of multiple and diverse source of data to examine phenomenon within its context.[113] Yin defines a case study as "*an empirical enquiry that investigates a contemporary phenomenon in-depth and within its real-life contact, especially when the boundaries between phenomenon and context are not clearly evident*".[114] The thesis uses a comparative case study analysis as this allows an in-depth analysis to examine the motivations of donor countries to invest in cyber capacity building, and specifically to what extent these investment decisions are driven by the internet governance divisions. The advantage of using multiple case studies is that it allows the opportunity to compare and contrast the findings and the evidence created is stronger and more reliable than from a single case study.[115] Nevertheless, these deficiencies are countered through triangulation of diverse data sources as well as methodological triangulation, which will be explained below in section 3.2 and 3.3. The case study selection is presented below in sub-section 3.6.

3.2 Data sources

Triangulation of data sources allows for a "*thick description of the phenomenon under scrutiny*".[116] The primary data sources that will be used for the thesis includes voting data from

[113] Pamela Baxter and Susan Jack, "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers," *The Qualitative Report* 13, no. 4 (December 1, 2008): 544–59, https://doi.org/10.46743/2160-3715/2008.1573.

[114] R.K. Yin, *Case Study Research: Design and Methods*, 4th ed. (Thousand Oaks, CA: Sage Publications, 2009), 46.

[115] Johanna Gustafsson, "Single Case Studies vs. Multiple Case Studies: A Comparative Study," 2017, https://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf.

[116] Andrew K. Shenton, "Strategies for Ensuring Trustworthiness in Qualitative Research Projects," *Education for Information* 22, no. 2 (2004): 63–75, https://doi.org/10.3233/EFI-2004-22201.

the UNGA resolutions on cyber-related issues, project data on cyber capacity building activities, interviews with twelve representatives from donor countries, policy documents and reports. Additionally, the secondary data sources that this thesis will use are journals, articles, and web pages. Besides the triangulation of data sources, this thesis will also use triangulation in its data collection as explained in the next section.

3.3 Methods of data collection and justification

Triangulation of methods of data collection supports the notion that using more than a single method will allow the understanding of issues from different perspectives in qualitative research.[117] Therefore, the methods of data collection can be identified as triangulation 'within-method' through the semi-structured interviews with twelve representatives from four different donor countries to ensure internal consistency and cross-checking; as well as 'between-methods' through the application of multiple data collection methods.[118]

3.3.1 Open-source databases

First, the thesis will collect data through desk research using open-source databases, more specifically the UN voting database[119] and Cybil – the CCB knowledge portal[120]. In order to test the hypothesis, the thesis will need to collect data to assess if countries have changed their position in the internet governance debate by analyzing the voting behavior of countries during five UNGA resolutions on cyber-related issues between 2018-2020. This allows an assessment on where countries stand in the internet governance debate. Analysis through the UN voting database allows research on the influence of development aid as done so by other researchers.[121] Therefore, this thesis uses voting data from the following UNGA resolutions: A/RES/73/27; A/RES/73/266; A/RES/73/187; A/RES/74/247; and A/RES75/240. Moreover, Cybil[122] is used in this thesis as a central repository to obtain information on cyber capacity building projects.

[117] "Methodological Triangulation in Qualitative Research In: Doing Triangulation and Mixed Methods," 2018, https://doi.org/10.4135/9781529716634.

[118] Todd D. Jick, "Mixing Qualitative and Quantitative Methods: Triangulation in Action," *Administrative Science Quarterly* 24, no. 4 (1979): 602, https://doi.org/10.2307/2392366.

[119] "UN General Assembly: Voting Records Search," accessed November 20, 2021, https://www.un.org/en/ga/documents/voting.asp.

[120] "Cybil Portal," accessed August 30, 2021, https://cybilportal.org/projects/.

[121] Zielinska, "Development Diplomacy. Development Aid as a Part of Public Diplomacy in the Pursuit of Foreign Policy Aims: Theoretical and Practical Considerations."

[122] Cybil is a repository that is continuously updated – this thesis considers all project data in Cybil by 15 November 2021.

More specifically, project data of a selected group of countries to gain insights on whether they receive cyber capacity building support and from which donor countries.

3.3.2 Semi-structured interviews

Secondly, the primary data sources will be provided through the method of semi-structured interviews. Semi-structured interviews are a valuable method to collect qualitative, open-ended data, to delve into an interviewee's beliefs, perceptions, and attitudes towards a certain topic, and to explore sensitive issues.[123] This thesis will conduct semi-structured with representatives of donor countries through a set of questions that will be asked to each respondent. The aim is to conduct interviews with donor countries who support the multi-stakeholder approach of internet governance, in order to do a comparative analysis regarding their incentives for their cyber capacity building efforts. As mentioned above, this is in line with triangulation within-method to ensure internal consistency and cross-checking. Therefore, interviews were conducted with twelve respondents, by interviewing three representatives from four donor countries. Due to the small-N of the interviews, there was not a coding strategy applied to the responses. By conducting interviews with three representatives per country, the thesis follows the triangulation within-method to ensure reliability and validity of the results. Furthermore, the interviews were conducted virtually as the respondents are located across the world. The interviews took place via Microsoft Teams and were recorded to the knowledge of the respondents. Due to sensitive topic of this thesis, the respondents are anonymized, and the transcripts are not made available in the thesis, but the relevant data will be presented in the analysis section and the interview guide is available in Annex.

3.3.3 Documents

Thirdly, documents will be used to support the data gathered from the semi-structured interviews when respondents refer to them. This includes policy documents and policy reports, from both international processes on cyber-related issues as well as key documents that outline a donor country's ambitions regarding cyber and foreign policy.

[123] Melissa DeJonckheere and Lisa M Vaughn, "Semistructured Interviewing in Primary Care Research: A Balance of Relationship and Rigour," *Family Medicine and Community Health* 7, no. 2 (March 1, 2019): e000057, https://doi.org/10.1136/FMCH-2018-000057.

3.4 Ethics

Cybersecurity is a sensitive topic. This is especially true in the international arena regarding the internet governance debate as this is a sensitive issue vis-à-vis the larger geopolitical debate. Therefore, this thesis has several ethical considerations. First, this thesis focuses on one side of the internet governance debate, the position that favors an open, free, secure internet through a form of multi-stakeholder governance. This decision was taken due to the availability of (English) discourse, open and accessible information about their cyber capacity building projects, and accessibility to representatives from these donor countries. Additionally, the transparency and knowledge of cyber capacity activities is much larger and organized, compared to potential cyber capacity efforts of the other "sovereign and controlled" side. Secondly, the thesis touches upon a politically sensitive issue and therefore it will be a challenge to get a complete understanding of the exact drivers behind cyber capacity building investments, since not all information is allowed to be shared by the respondents in the interviews. Therefore, the analysis is not solely dependent on the donors' narrative, but also considers the actual actions (cyber capacity activities). Lastly, since empirical research on this topic is challenging due to a lack of trust and transparency on the topic of cybersecurity, the responses of the donor countries will be anonymized in the analysis.

3.5 Delimitations and limitations

Every research study has its limitations and delimitations, and this thesis is not an exception. Starting with the delimitations. First, the choice was made for a qualitative research methodology through a comparative case study of donor countries that are active in cyber capacity building and support a multi-stakeholder governance. The risk with small-N case studies is the lack of external validity and that they do not explain broad patterns. Nevertheless, the study of a limited number of donor countries can still provide very valuable insights and through triangulation within- and beyond methods, this thesis attempts to increase the validity of the results. The second delimitation is the case selection of the donor countries. There is diversity in the scale and number of cyber capacity building activities conducted due to differences in available budgets, their influence in the respective regional and international arena, and therefore there is likely a limitation on how their cyber capacity building efforts is driven by their foreign policy objectives. Nonetheless, the intentional choice was made to focus on four donor countries that target different regions with their cyber capacity building activities, and that could be considered to have comparable influence in the international arena based on how they advocate their position in the internet governance debate. The third delimitation is connected to the narrowing down of the scope of this study to the international cyber capacity building investments by donor countries and does not focus on the investments made by others, for example the World Bank, ITU, and regional organizations. This decision was made since the focus of this study is to examine the link on the foreign policy objectives from countries as driver for their cyber capacity building investments. Hence, this is not applicable for the international and regional organizations. Suggestions for future research concerning these stakeholders is included in the discussion part of this study.

Additionally, the thesis has several limitations. First, as mentioned in the Ethics section, the thesis only focuses on the cyber capacity building investments from countries supportive of the 'multi-stakeholder' governance perspective, since the transparency and knowledge of cyber capacity building activities is much larger and organized, compared to potential cyber capacity efforts of the other side within the internet governance debate. This will also be considered in the suggestions for future research to examine how the other camp conducts cyber capacity building, and if their drivers are linked to the internet governance debate divisions. Secondly, although Cybil is the single open-source database with information on countries cyber capacity building projects, it is limited as it is dependent on information volunteered by stakeholders. Therefore, not all projects might be included as some stakeholders do not submit new or updated information on ongoing cyber capacity projects and some country recipients do not want all the projects published. Nevertheless, since Cybil is the only available database with this type of data and has also been used in other (recent) academic research, the choice is made to still use Cybil as a source in the analysis.

3.6 Case study selection

The countries that are selected for the comparative case study are donor countries that are on the 'multi-stakeholder side' of the internet governance debate; meaning they favor an open, free, secure internet. To make the case study selection, the thesis used the 'Digital Deciders mapping tool' developed by New America.[124] They scored all countries on five factors: internet values, political values, international internet policy participation, international influence, and internet reliance score. Through ranking all countries, four categories were identified: Global & Open, Sovereign & Closed, Digital Deciders, and LDC or Small Country. The countries that

[124] New America, "The Digital Deciders - Mapping Tool," 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/understanding-the-clusters-through-data/.

were identified as Global & Open were cross-checked to see if they are active in cyber capacity activities by project data available on Cybil.

Next, the thesis examined any ongoing cyber capacity building projects linked to the UN dialogue for the selection of the countries. The Women in Cyber Fellowship project[125] is a running project to increase the number of female country representatives in the UN dialogues, for example the OEWG. This project was started by Australia, Canada, the Netherlands, New Zealand, and the United Kingdom – and the United States recently also joined this effort. This project was key in the case selection, since it is 1) a multi-year project with various donors; 2) each donor contributes according to their own resources and mandate; 3) directly increases the participation of (female) Global South country representatives in the UN First and Third Committee processes, and most importantly 4) the fellows as beneficiaries in the project have a direct influence in the shaping and voting of UNGA resolutions on cyber-related issues. In sum, the case study selection was based on the above factors, their available project information on Cybil, and availability of respondents.

Therefore, the following donor countries are selected: Australia, Canada, the Netherlands, and the United Kingdom. Table 2 demonstrates their ranking and their score according to the Digital Decider mapping tool as well as the number of cyber capacity activities available of Cybil.

Table 2: Case study selection donor countries

	Digital Deciders mapping tool		**Cybil**
	Ranking	*Score*	*# of CCB activities*
Australia	3	0.882	84
Canada	2	0.885	14
The Netherlands	8	0.857	25
United Kingdom	1	0.908	211

The author of this study approached the Ministry of Foreign Affairs since the scope of the study is linking capacity building efforts with foreign policy objectives. The four donor countries selected their three representatives to be interviewed for this thesis. All respondents work on cyber capacity building efforts within their Ministry of Foreign Affairs; they are either involved in policymaking, project implementation (e.g., Women in Cyber Fellowship), and/or involved in the UN dialogue. The respondents are anonymized, and the transcripts are not made available

[125] "Women in Cyber Fellowship - Cybil Portal," accessed November 4, 2021, https://cybilportal.org/projects/women-in-cyber-fellowship/.

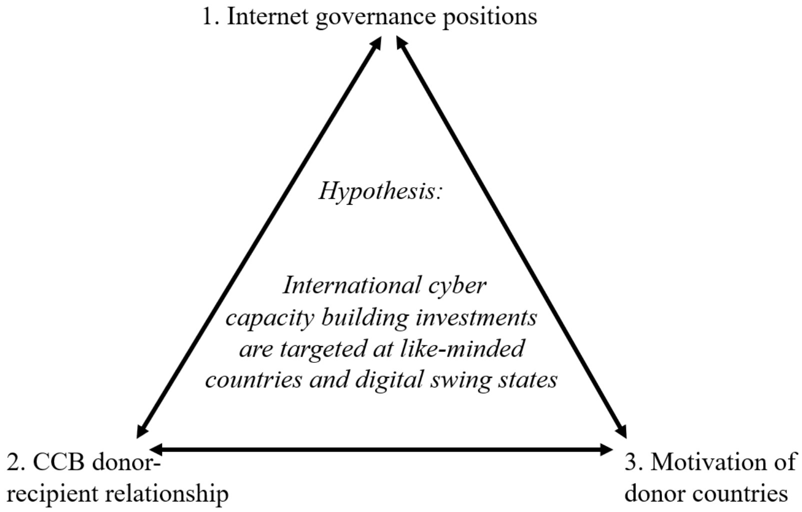
in the Annex of the thesis, due to the sensitive topic. The respondents will be referred to by the acronym of their country and the number 1-3.

3.7 Analytical framework

The research design section will conclude with the presentation of this study's analytical framework that will be applied in the analysis of the study. The analytical framework is visualized in Figure 1 and further explained below. The analysis of the thesis will be divided into three categories according to the three remaining sub-research questions to test the hypothesis: *International cyber capacity building investments are targeted at like-minded countries and digital swing states*. The remaining sub-research questions are:

- What are the internet governance divisions in the international arena?
- Which countries receive cyber capacity support from donor countries?
- What are the motivations of countries to invest in Cyber Capacity Building activities?

Figure 1: Analytical framework of the thesis


1. Internet governance positions
Hypothesis:
International cyber capacity building investments are targeted at like-minded countries and digital swing states
2. CCB donor-recipient relationship
3. Motivation of donor countries

First, through an analysis of the UNGA resolution voting between 2018-2020 on cyber-related issues, a stakeholder mapping will be presented with an overview on where the UN member states stand in the internet governance debate. This will help determine whether the groups align with the "multi-stakeholder and open" group, the "sovereign and controlled" group, or if they belong to the group of the digital swing states. This will lead to the second part of the analysis, where the hypothesis is tested to determine if like-minded countries and digital swing states receive cyber capacity building investments from "multi-stakeholder and open" donor countries through an analysis of cyber capacity building projects on Cybil. The third and final part of the analysis will focus on the motivation of donor countries in cyber capacity building investments by an examination of the twelve respondents from the four like-minded countries.

4. Empirical analysis

The empirical analysis of the thesis focuses on answering the three remaining sub-research questions. The first part will focus on what the evidence is of the internet governance divisions in the international arena and by doing so identifying the group of countries that are potentially interesting for cyber capacity building investments according to this thesis's hypothesis: *International cyber capacity building investments are targeted at like-minded countries and digital swing states.* Secondly, by using the Cybil database, this thesis will explore whether donor countries are interested in specific countries with regards to cyber capacity support. Lastly, the empirical analysis will examine what the motivations are of countries to invest in international cyber capacity building activities through a set of interviews with four countries that invest in these activities: Australia, Canada, the Netherlands, and United Kingdom.

4.1 The internet governance divisions in the international arena

First, as a starting point, before exploring the hypothesis of this thesis, this section will focus on answering the second sub-research question of the thesis: what are the internet governance divisions in the international arena? This will determine where the different countries stand in the internet governance debate, which is necessary for the remainder of the analysis. The analysis of UN voting data can demonstrate common interests of states regarding cyber-security related topics.[126] Over the past decades, between 2018-2020 there have been five cyber-related UNGA resolutions that required voting,[127] which can be used as indicators of where countries stand in the internet governance debate, as is demonstrated in Figure 2[128] on the next page.

4.1.1 Voting in the UNGA resolutions and identified categories

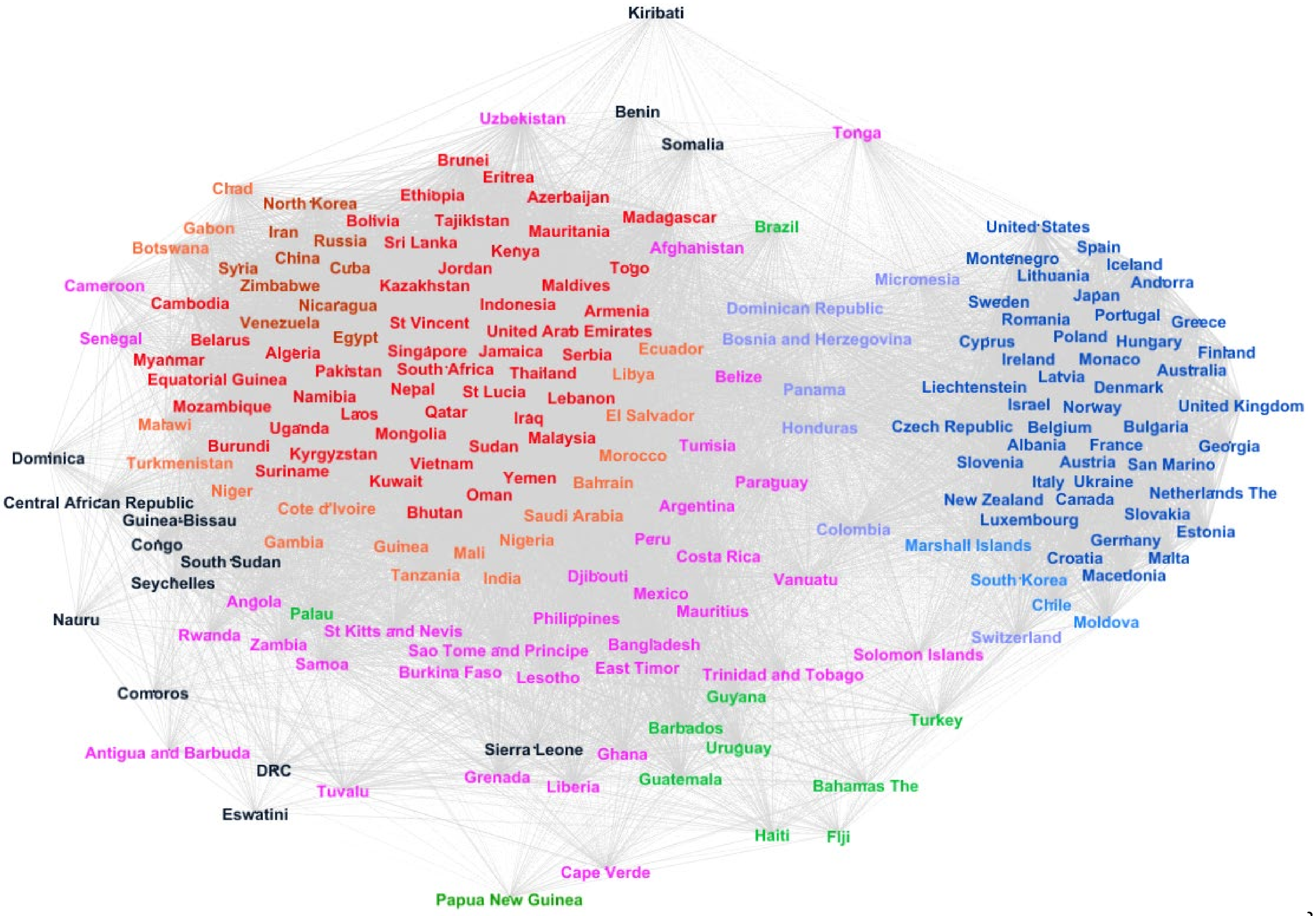
Within UNGA resolutions, each UN Member state (193 in total) have four possibilities for voting: they can vote 'yes' in favor of the resolution; they can vote 'no' against the resolution, they can 'abstain' from voting by not taking a position; or they did not participate in the voting

[126] Robert Collett has used the UN voting data from the five UNGA resolutions and the 2012 WCIT voting record to visualize complex voting histories. He presents dynamic network graphs and diagrams as a tool for researchers and diplomats in cyber diplomacy to analyze trends, patterns and relationships on how the voting of countries has been consistent or has changed over the years: https://cybercapacity.org/new-way-to-visualise-un-cyber-diplomacy-voting-records/.

[127] The UNGA resolutions that are used for this mapping are: A/RES/73/27; A/RES/73/266; A/RES/73/187; A/RES/74/247; and A/RES75/240. These UNGA resolutions are explain in section 2.1.

[128] Figure 2 is created by the author using the tool Gephi, based on the UNGA resolution voting records that are mentioned in footnote 126, an overview is included in Annex 1 on page 70.

Figure 2: Stakeholder mapping of connections of countries' voting behavior in UNGA resolutions related to cyber issues



altogether, implying that their vote is 'void'.[129]

Therefore, based on the voting behavior of the 193 UN Member States, in total nine types of behavior can be identified that can be grouped in three categories: 1) "Multi-stakeholder and open"; 2) "Sovereign and controlled"; and 3) "Digital swing states". The first category is the "multi-stakeholder and open" group, including the blue countries on the right side of Figure 2, demonstrate the group of countries that have similarly voted throughout all five votes. The countries in light blue and purple have voted respectively four and three times in the same way as this group. Secondly, on the left side of the map, the dark red countries, are part of the group of countries that call for a more "sovereign and controlled" internet; these countries have voted five times in a similar way. The countries in bright red and orange have voted respectively four and three times in the same way as this group. The third category included the digital swing states. The countries in green have at least abstained three times for voting (Papua New Guinea – being the only country that abstained during all five votes). The countries in black have not participated in the voting at least three times. Lastly, the countries in pink have voted differently throughout the five resolutions, sometimes siding with the one group, other times with the other, and often refrained from voting or abstained. Table 3 below outlines the three different groups, and Figure 3[130] on the next page demonstrates the global map with these nine different categories that demonstrates both the regional and global divisions. [131]

Table 3: Categories of countries voting behavior in five UNGA resolutions related to cyber

"Multi-stakeholder & open"	"Sovereign & controlled"	"Digital swing states"
• NYNNN	• YNYYY	• AAA(AA)
• 4x NYNNN	• 4x YNYYY	• VVV
• 3x NYNNN	• 3x YNYYY	• Mix

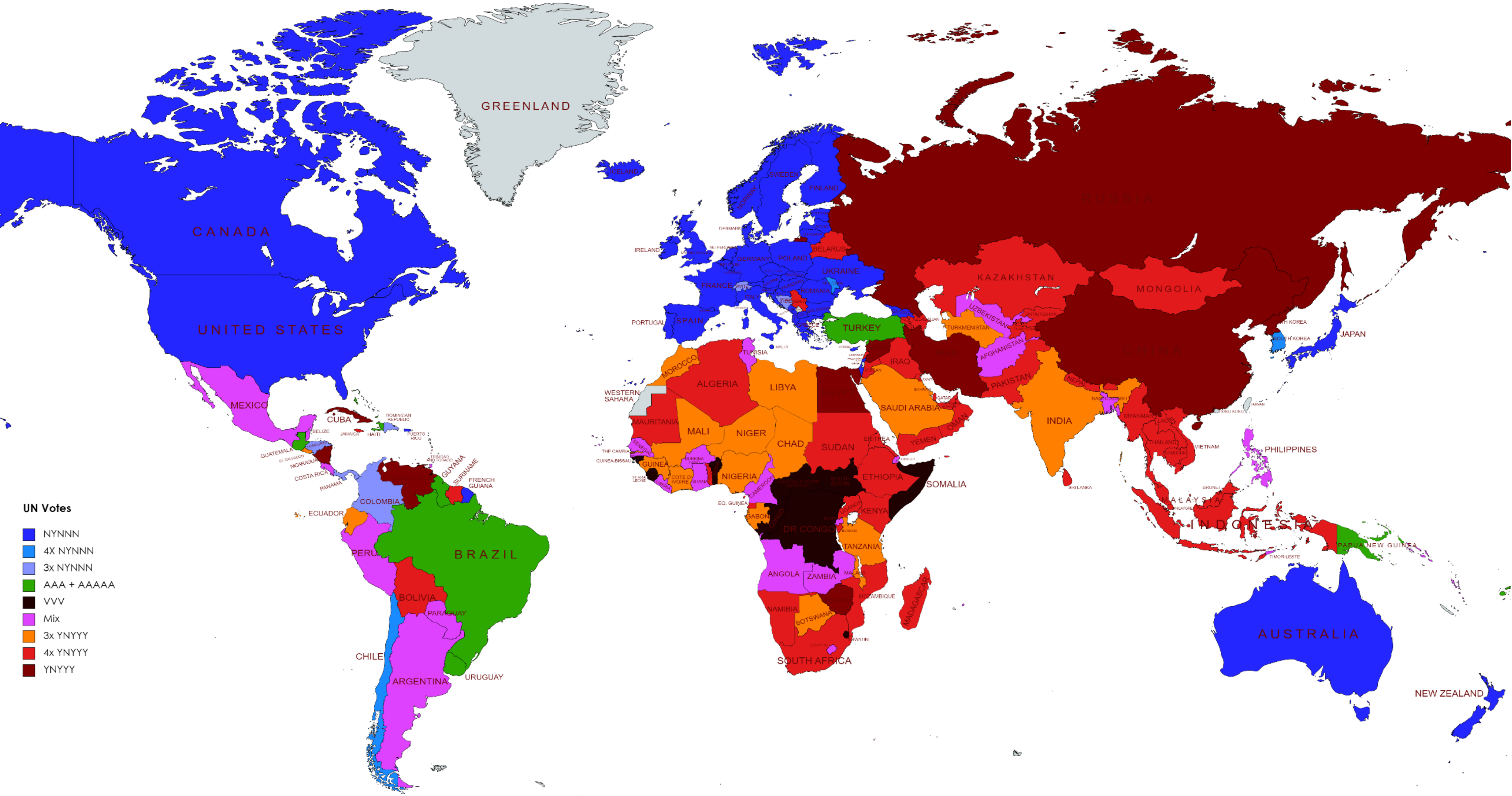
The next sections will analyze the countries in the three categories and highlight any findings in the voting.

[129] This thesis highlights the difference between an abstained vote and a void vote. The abstained vote can imply that a country does not want to take a side, whilst the reasons for a void vote can range from being a political tactic as well as that the delegation of the respective vote was absent during the vote. Therefore, the abstained vote is a deliberate neutral vote – and the void votes are being considered as a pattern in this thesis when they have occurred three out of five times.

[130] Figure 3 is created by the author using the same database as Figure 2 through mapchart.net.

[131] Annex 1 demonstrates an overview of how each country voted, since this is not visible in not all countries are visible in Figure 3, for instance the Caribbean and Pacific islands.

Figure 3: Map of countries' voting behavior in UNGA resolutions related to cyber issues (2018-2020)



4.1.2 The "multi-stakeholder and open" group

First, to start with the NYNNN group, this includes the 27 European Union (EU) Member States and other Western countries, for instance Australia, Canada, Israel, UK, and the USA that are all OECD members.[132] Interestingly, this group also includes a number of Balkan countries such as Albania, Montenegro, North Macedonia and from the EU's Eastern Partnership: Georgia and Ukraine. Additionally, several small countries within Europe also belong to this group: Andorra, Liechtenstein, Monaco, and San Marino, as well as Iceland and Japan. In total this is a group of 45 countries that has voted in a similar way through the five votes.

Secondly, the four countries that voted 4x NYNNN, either abstained (Chile, Moldova, and South Korea) or did not participate in the voting (Marshall Islands) during one vote. Most interesting in this category are Chile, the first and only country from Southern America to vote in this similar manner, and the Marshall Islands, as the only Pacific Island country. Moldova is one of the Balkan countries with close relationship to the EU through the Eastern Partnership. South Korea is, similar to Japan, one of the Western countries in Asia.

Thirdly, the group that votes three times in a similar way, includes amongst others Switzerland – who abstained during the two UNGA resolutions that initiated the OEWG and extended the same initiative, which is chaired by the Swiss. A number of Southern American countries (Dominican Republic, Honduras, and Panama) voted the two other times favorable for the two OEWG UNGA resolutions that the other countries opposed; Colombia voted the first time in favor and abstained on another resolution. Bosnia and Herzegovina followed the same pattern as the Southern American countries. Interestingly again, Micronesia, another Pacific Island country, did not participate in two of the five votes – again the votes on the Russian-sponsored OEWG resolutions.

In sum, with a few exceptions, these 56 countries represent mostly 'Western countries', and their views on internet governance are clearly reflected in their voting. Although this group is first referred to as the "multi-stakeholder and open" internet group, for the remainder of the thesis, this group will be referred to as "like-minded countries".

[132] "List of OECD Member Countries ," accessed December 4, 2021, https://www.oecd.org/about/document/ratification-oecd-convention.htm.

4.1.3 The "sovereign and controlled" group

First, the core of the "sovereign and controlled" internet group, the group that voted five times the same way, is quite smaller than the core group of the other camp. This group represents ten countries, spread globally across all continents that desire more sovereign control over the internet: China, Cuba, Egypt, Iran, Nicaragua, North Korea, Russia, Syria, Venezuela, and Zimbabwe.

Secondly, the group that voted four times in a similar way as dark red group, are in total 49 countries that are red in the stakeholder mapping. From these 49 countries, 35 countries, voted also in favor of the re-establishment of the UNGGE back in 2018 after also voting in favor of the establishment of the OEWG – these countries were in favor of two similar parallel processes. Bolivia was the only country that voted against the re-establishment of the UNGGE, similar to the dark red group. The other countries either abstained or did not participate in the vote.

Thirdly, the 19 orange countries that voted three times in a similar way are also spread globally. From this group 11 voted in favor of the re-establishment of the UNGGE as well as the establishment of the OEWG. They abstained or did not participate in the last two votes. The other 8 either abstained or did not participate in two of the five votes. In sum, these 78 countries are grouped under the "more controlled internet" group as they voted at least three times or more in a similar way as the dark red group. This group will not be further elaborated on in the thesis, as this group is outside of the hypothesis' scope.

4.1.4 The "digital swing states"

The last category of countries, which is highly relevant for this thesis, are the countries that this thesis identifies as the digital swing states through their voting behavior during the five UNGA resolutions related to cyber issues. This category includes the countries that either abstained at least three times, did not participate in the voting at least three times, and countries that do not follow a pattern but have voted at least three different ways.

First, the group that abstained at least three times includes 11 countries. The most interesting case here is Papua New Guinea that is the only country that abstained during all five votes. Additionally, the Bahamas abstained four times, joining the "like-minded countries" in the only yes vote on the UNGGE. Another observation is that most countries are small island nations:

Bahamas, Barbados, Fiji, Haiti, Palau, and Papua New Guinea. The other countries are Southern American countries: Brazil, Guatemala, Guyana, and Uruguay. The exception, and an interesting case, is Turkey, which abstained three times, and voted the other two times similarly as the like-minded countries. Another observation from this group is that both Fiji and Haiti abstained three times, did not participate in a vote once, and voted in favor of the re-establishment of the UNGGE.

Secondly, the group of 14 countries that did not participate in the voting at least three times, that are marked black in the stakeholder mapping. This includes mostly African countries: Benin, Central African Republic, Comoros, Democratic Republic of Congo, Eswatini, Guinea Bissau, Seychelles, Sierra Leone, Somalia, and South-Sudan; and two Pacific Island countries: Kiribati and Nauru. As mentioned above, the non-participation in the voting can either be a strategic decision (not wanting to choose side, they do not see the importance, or that they were unable to participate in the voting. However, since these countries did not vote at least three times (Dominica and Eswatini even four times), it could be argued that it is more likely one of the first two reasons rather than the latter.

Thirdly, the remaining 34 countries voted in a ‘mixed’ manner during the voting, not favoring any side, often with multiple abstentions or void votes. When analyzing these votes, one observation that can be made is that these group of countries almost never voted against a resolution. For example, when considering the first two resolutions in 2018 regarding the OEWG and UNGGE, most countries voted in favor for both UNGA resolutions, abstained or did not participate in the vote for either. Therefore, this group is also a separate category in the digital swing states. This group will be examined in more detail together with the like-minded group in the next section regarding their cyber capacity building activities.

4.1.5 Conclusion on internet governance divisions

In conclusion, this section used the voting behavior of the 193 UN Member States during five cyber-related UNGA resolutions to map the internet governance divisions in the international arena. Three main categories were identified with nine types of voting behavior. As is demonstrated in stakeholder mapping and the world map visuals, the groups are scattered both regionally and globally, except for Europe. The group of 59 digital swing states is quite large, and therefore convincing these countries to join a certain camp could be a game changer for possible future resolutions. The hypothesis of this study states that *international cyber capacity* *building investments are targeted at like-minded countries and digital swing states.* Therefore, the remainder of this study's analysis will focus on the six types of groups across the two categories: like-minded and the digital swing states. These are the countries outlined in Table 4 below. The next section of the analysis will examine whether cyber capacity building investments from donor countries are targeted at these like-minded countries and digital swing states.

Table 4: Overview of 'like-minded countries' and 'digital swing states'		
56 'Like-minded countries'	**NYNNN**	Albania, Andorra, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, New Zealand, N-Macedonia, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, Ukraine, UK, USA
	4x NYNNN	Chile, Marshall Islands, Moldova, South-Korea
	3x NYNNN	Bosnia and Herzegovina, Colombia, Dom. Republic, Honduras, Micronesia, Panama, Switzerland
59 'Digital swing states'	**AAA(AA)**	Bahamas, Barbados, Brazil, Fiji, Guatemala, Guyana, Haiti, Palau, PNG, Turkey, Uruguay
	VVV	Benin, CAR, Comoros, Congo, Dem. Rep. of Congo, Dominica, Eswatini, Guinea Bissau, Kiribati, Nauru, Seychelles, Sierra Leone, Somalia, South Sudan
	Mix	Afghanistan, Angola, Antigua and Barbuda, Argentina, Bangladesh, Belize, Burkina Faso, Cabo Verde, Cameroon, Costa Rica, Djibouti, Ghana, Grenada, Lesotho, Liberia, Mauritius, Mexico, Paraguay, Peru, Philippines, Rwanda, St. Kitts and Nevis, Samoa, Sao Tome and Principe, Senegal, Solomon Islands, Timor-Leste, Tonga, Trinidad and Tobago, Tunisia, Tuvalu, Uzbekistan, Vanuatu, Zambia

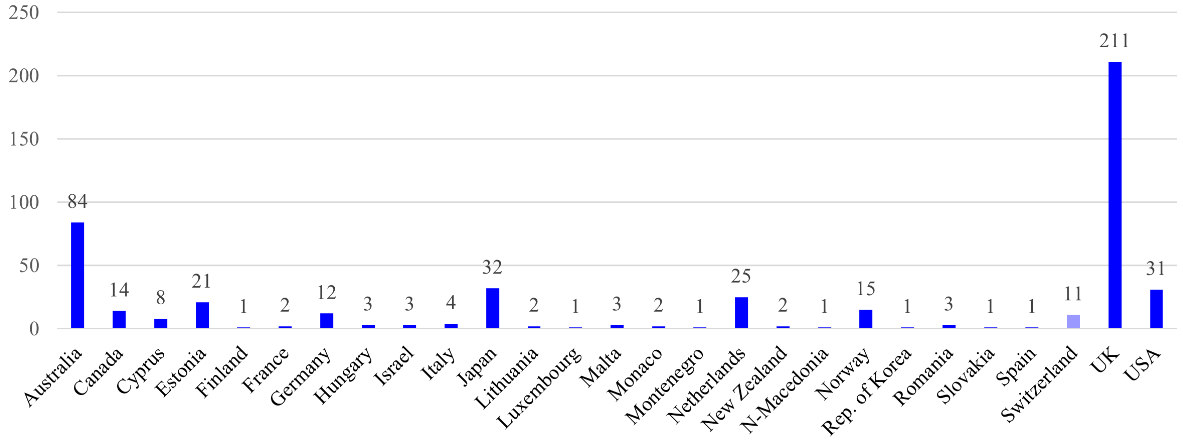
4.2 Exploring the target countries of cyber capacity support by donor countries

The second part of the analysis will explore whether donor countries are interested in specific countries with regards to cyber capacity support by using the available project information on Cybil. More specifically, the focus will be on the countries identified in Table 4 as 'like-minded countries' and 'digital swing states', in order to answer the sub-research question: which countries receive cyber capacity support from donor countries? This section will first identify which countries are the cyber capacity donors based on the like-minded table in the section above.[133] Next, the cyber capacity building activities in the 'like-minded countries' will be examined and after the activities in the 'digital swing states' countries. In the conclusion of this section, the sub-research question will be answered.

4.2.1 Identifying the donor countries in cyber capacity building

First, the analysis in 4.1 identified 56 countries in the 'like-minded countries' category. When examining these countries on Cybil, from this group there are 27 countries who fund cyber capacity building activities. From these 27, there are 25 countries in the core group – the NYNNN, and additionally the Republic of Korea and Switzerland are identified as countries that invest in cyber capacity building as presented in Figure 5. Nonetheless, the number of cyber capacity building activities that these countries engage in varies enormously. For example, according to Cybil, countries as Finland, Luxembourg, Montenegro, North Macedonia, Republic of Korea, Slovenia, and Spain are involved in one cyber capacity project. Whilst in comparison, Australia is listed as a donor country in 84 activities, and the United Kingdom even in 211.

Figure 4: # cyber capacity projects by donor countries on Cybil



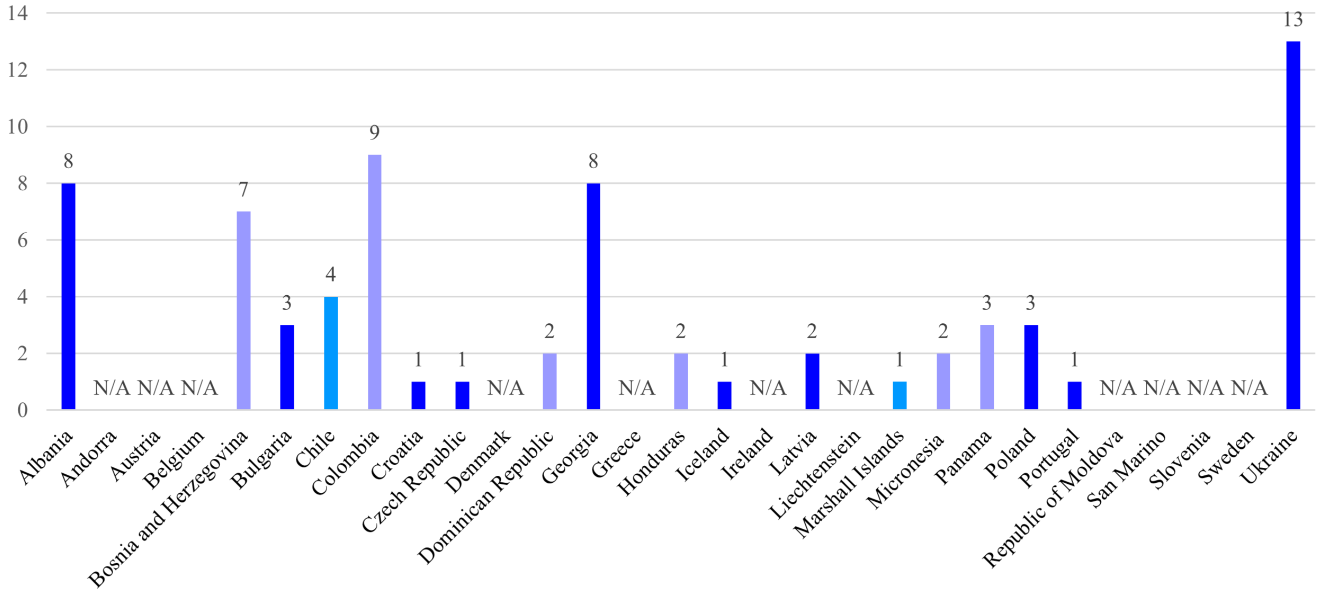
[133] Cybil does not provide information on the budget of the cyber capacity projects, therefore the analysis in this section is not focused on the amount of cyber capacity investments. The focus of this section is the selection of recipient countries by donor countries for cyber capacity support.

The identification of the donor countries will support the next part of the analysis as these countries will be excluded, since they are not recipient countries of cyber capacity building.[134] Therefore, the next section will focus on the remaining 88 like-minded countries and digital swing states in the next section.

4.2.2 Cyber capacity building activities in 'like-minded countries'

This section will focus on how many cyber capacity building investments from donor countries are targeted at the remaining 29 'like-minded countries'. Figure 6 visualizes the countries that receive cyber capacity building support from donor countries as well as the number of activities. The first observation that can be made is that a high number of countries have N/A (not applicable) listed. There could be two reasons for this. First, it can refer to that the country does not receive any cyber capacity support, because the country already has a sufficient cyber maturity and/or does not require external resources through development aid to assist in increasing its cyber maturity.

Figure 5: # of cyber capacity activities received in like-minded countries



A second reason for the N/A listing is that a country does receive cyber capacity support; however not from any donor countries, but from international and/or regional organizations. Therefore, it is not applicable for this study and analysis. In the case of the countries above in Figure 6, they do receive cyber capacity support, not from donor countries but mainly from the

[134] Within Cybil, these countries can be a beneficiary – often through cyber capacity building activities that target an entire region. For example, the OAS as multiple activities for all of the OAS member states, which includes Canada and the US, who fund these projects. Therefore, for the purpose of this thesis, if a country funds cyber capacity building activities, they are no longer considered a recipient.

EU, which has multiple cyber capacity activities targeted at all its Member States. The one exception is the Republic of Moldova, Cybil does not have any information of cyber capacity activities in this country.

Based on this overview, a few countries really jump out: Albania, Bosnia and Herzegovina, Colombia, Georgia, and Ukraine receive the most cyber capacity support, between 7-13 activities. The UK is active in all five of these recipient countries in one or multiple projects. The other donor countries are Canada, Estonia, Germany, Finland, the Netherlands, Republic of Korea, Spain, and the US. The European donor countries are focused on Albania, Bosnia and Herzegovina, Georgia, and Ukraine; whilst Colombia receives support from Canada, Estonia, Spain, UK, and the US. Colombia is interesting in this case, since it seems more a country of regional interest for Canada and the US, than for the European countries. However, the UK is involved in each region, Estonia has many cyber capacity activities on the topic of e-governance,[135] where Estonia is well known for, and Spain has historical and linguistic ties to Colombia. The Republic of Korea demonstrates an interest in the Balkan countries, with cyber capacity activities in Albania as well as Bosnia and Herzegovina.

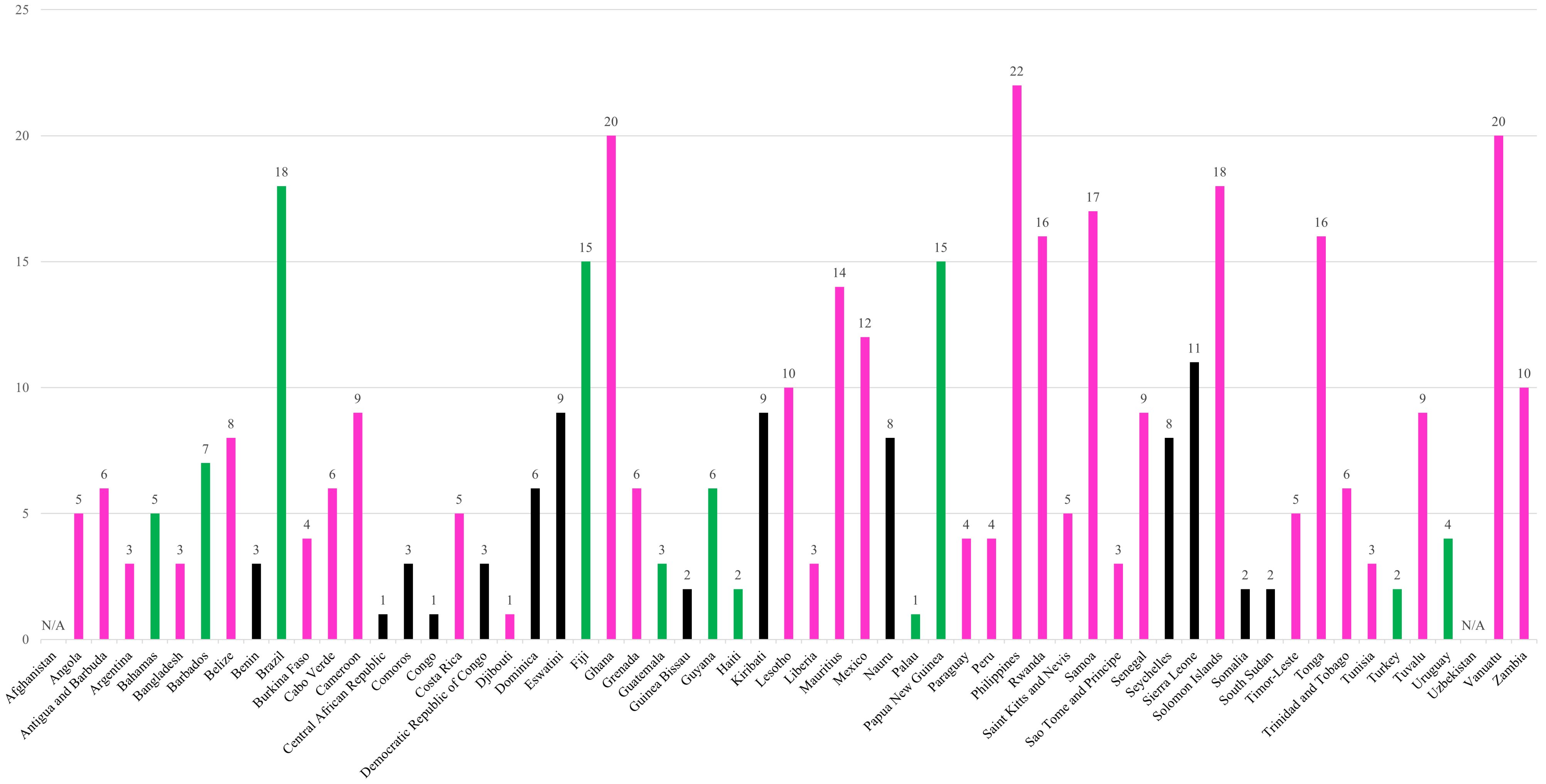
In sum, from the 29 like-minded countries, there are five countries that receive above average cyber capacity building investments from the donor countries: three countries voted similar as the NYNNN group, and two countries voted three times in this manner. There are multiple donor countries active in these countries. Several arguments can be linked to their interest to those countries, most evidently regional ties can be identified as well as historical ties. However, not all of the donor countries' interests in some of the recipients is self-evident.

4.2.3 Cyber capacity building activities in 'digital swing states'

This sub-section will focus on how many cyber capacity building activities from donor countries are targeted at the 59 'digital swing states'. Figure 7, on the next page, demonstrates how often these countries can be identified as a recipient of cyber capacity building support from donor countries. Interestingly, 57 of the 59 countries receive cyber capacity building support from donor countries. The two exceptions are Afghanistan and Uzbekistan, who do receive capacity building support but not from countries directly, but from respectively the

[135] "Cybil Portal - Estonia Projects," accessed November 20, 2021, https://cybilportal.org/projects/?_sfm_funders_relationship=2844-%2C-765.

Figure 6: # of cyber capacity activities received in digital swing states



World Bank and OSCE. In section 4.1, the category digital swing states was divided into the three groups: mostly abstentions (AAA), mostly void votes (VVV), and the mixed voting that sided with either sides and/or abstained or did not vote (Mixed). When examining these three groups in the chart, no observation can be made whether one group is more interesting for cyber capacity building activities compared to the other. Some of the green AAA group received many cyber capacity building activities compared to others in the group, for example Brazil, Fiji, and Papua New Guinea, whilst others only received one or two cyber capacity activities. The same goes for the Void group, where Eswatini, Kiribati, Nauru, Seychelles, and Sierra Leone received the most support, whilst others received much less support. From the Mixed voting group, Belize, Cameroon, Ghana, Lesotho, Mauritius, Mexico, the Philippines, Rwanda, Samoa, Senegal, Solomon Islands, Tonga, and Tuvalu received the most support, while others received much less support.

When examining the digital swing states that received the most cyber capacity activities closer; it becomes apparent that almost all countries receive cyber capacity support from at least three or four different donors or even more. The exceptions are the Pacific Islands: Fiji, Kiribati, Nauru, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu that receive almost all of their cyber capacity support from Australia and to a lesser extent from the UK, and in some countries, Estonia has conducted one or two activities. Similar to Colombia, it is Canada, Estonia, the UK, and the US who invest in Brazil's cyber capacity building, whilst in Mexico it is Canada, Estonia, Japan, Spain, and the UK. Another observation that can be made is that there are 11 donor countries active in the African region: Estonia, Germany, France, Japan, Republic of Korea, Luxembourg, the Netherlands, Norway, Switzerland, the UK, and the US. Most donor countries are also active in the same countries. Perhaps the most interesting case from the digital swing states is the Philippines, which is listed highest with 22 cyber capacity activities, but also has the most donor countries, including countries from the "sovereign and controlled" camp: Australia, Cambodia, China, Japan, the Netherlands, Singapore, the UK, and the US. There are not many cyber capacity activities on Cybil that are funded by China and Cambodia, therefore it is interesting to see that they are also conducting cyber capacity building activities in digital swing states.

In sum, apart from two countries, all countries identified as digital swing states receive cyber capacity building investments from donor countries. In comparison with the like-minded countries, the digital swing states receive a far higher number of cyber capacity activities.

Although one of the reasons can be is that the cyber maturity is already higher in most of the like-minded countries, and that the digital swing states are often developing or LDCs, this is still relevant for this thesis. Moreover, apart from the Pacific, where Australia is the main donor, recipient countries in other regions have many different donor countries involved in cyber capacity building activities, especially countries in the African region.

4.2.4 Conclusion target countries of cyber capacity activities by donor countries

In conclusion, this section aimed to answer the sub-research question on which countries receive cyber capacity activities from donor countries. From the 56 like-minded countries, 27 could be identified as a donor country in cyber capacity building activities. Some of them are involved in lots of activities, for example the UK with over 200 activities, but most are involved in only a few. Whether this is due to limited information on Cybil, or whether they are actually only involved in a few activities, is unknown to this study. There are also eight other donor countries that are funding at least ten cyber capacity building activities. Further, the other sub-sections examined the like-minded countries and the digital swing states for certain patterns. More cyber capacity building activities are targeted at the digital swing states. However, there could be several reasons for this. One of these reasons is because they are on the fence regarding the internet governance debate, but other likely reasons are that these countries have low cyber maturity and are more in need for support since most are developing or least developed countries. Also, other conclusions can be drawn. Most donors are active in their “own” region, for example Australia and Canada have a strong regional focus in respectively the Pacific and the Americas, and multiple European countries have a focus on Eastern Europe, and Africa. However, there are also donors that are involved in many different regions, for example the UK and in lesser extent the US.

Therefore, the analysis in this section demonstrates that although digital swing states are often the target for cyber capacity building activities, a direct link between the internet governance divisions and the number of cyber activities cannot be made based on this. The analysis does, however, indicate that most donor countries are driven by the regional component, and in some instances also by historical ties. The next section of the analysis will explore more in-depth what the drivers are of countries to invest in cyber capacity building activities and to what extent this is linked to the internet governance divisions.

4.3 Motivations of countries to invest in cyber capacity building activities

The last section of the analysis will examine the fourth and last sub-research question, what the motivations are of countries to invest in cyber capacity building activities through a set of interviews with three representatives from each country that invest in cyber capacity activities: Australia, Canada, the Netherlands, and United Kingdom. First, an overview will be provided on how these countries are engaged in cyber capacity building. Secondly, the sub-section will focus what the drivers are for cyber capacity building investments. Thirdly, the observations will be discussed on how these countries view cyber capacity building to be linked to their foreign policy objectives and whether cyber capacity building can be used as a tool to influence a country's position in the internet governance debate. Lastly, their views on the future of cyber capacity building will be analyzed.

4.3.1 Position in the internet governance debate

Although the countries have been identified based on the case selection, and their UN voting behavior, as countries that support the 'multi-stakeholder governance' model regarding the internet; all respondents were asked where their country stands in the internet debate. All of the respondents highlighted the importance of the multi-stakeholder model in their response. The Netherlands, Canada, and Australia refer to the internet as "open, free, and secure". The UK also mentions an open, free, and secure internet, but adds an extra adjective, "peaceful" by describing the internet (UK1, UK2, UK3).

4.3.2 Engagement in cyber capacity building

From the four case studies, Australia has the most transparent and clear priorities, which are outlined in their International Cyber and Critical Technology Engagement Strategy from April 2021.[136] From the 15 topical areas identified in their strategy, six are highlighted as priority areas, amongst them is cybersecurity (AUS2 & AUS3). Also highlighted in their strategy is Australia's priority region – the Indo-Pacific – which is viewed as their regional neighborhood (AUS1), and it has the highest strategic importance for them (AUS3). Another example of how Australia engages in their cyber capacity building activities is through bilateral cooperation, for example the Memorandum of Understanding on Cyber Cooperation with Papua New Guinea.[137]

[136] Department of Foreign Affairs and Trade, *Australia's International Cyber and Critical Tech Engagement Strategy*, *Australian Government Department of Foreign Affairs and Trade*, 2021, https://www.internationalcybertech.gov.au/.

[137] "MOU Between Papua New Guinea and Australia Relating to Cyber Security Cooperation | Australian Government Department of Foreign Affairs and Trade," accessed November 20, 2021,

For the period 2017-2024, Australia has a budget of 74 million AUD available for cyber capacity building (AUS3) that is linked to ODA, which is approximately 46 million EURO over a period of eight years.

Canada focuses mostly on the Americas region with its cyber capacity building activities, about 90% (CAD2), but also has several global projects, although these are not all on Cybil yet (CAD3). The main reason for this is that the Americas are their region (CAD1). Additionally, Canada is active through multiple regional organizations, amongst others also on cyber capacity projects. Examples are Francophonie, Commonwealth, and the OAS (CAD1). Important topics that Canada focuses on are the application of international law in cyberspace, cyber diplomacy, gender, and multi-stakeholder approach in cyber capacity building activities (CAD2). Canada has a cyber capacity building budget of in total of 19 million CAD for ongoing projects on cybercrime and cybersecurity since 2015 that is not linked to ODA (CAD3), which is approximately 13 million EURO over a period of seven years.

The Netherlands is currently revising its international strategy that also covers its priorities for cyber capacity building engagement (NL1 & NL2). At the moment, the Netherlands engages in multiple regions through bilateral and regional cooperation, for example through regional dialogues with ASEAN, OAS, and the African Union (NL1). Also, the Netherlands funds the Global Forum on Cyber Expertise (GFCE) since 2015 and supports a program on cybercrime with UNODC (NL2). There are several cyber capacity topics prioritized by the Netherlands: cyber diplomacy, application of international law in cyberspace, cybercrime training, CSIRT and critical information infrastructure protection (CIIP), and coordinated vulnerability disclosure (NL2). The interview respondents did not reveal any information on the budget for cyber capacity building.

The United Kingdom has been active in the field of cyber capacity building since 2012 (UK2). They connect its cyber capacity building program to the 15 major policies that are linked to the UK National Cyber Security Strategy that will identify their objectives and priorities for cyber capacity building (UK1 & UK2). Due to the UK's historical association with the Commonwealth, those countries continue to be a priority for the UK's cyber capacity building efforts; these priorities can shift depending on a particular administration, for example at the

https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/mou-between-papua-new-guinea-and-australia-relating-to-cyber-security-cooperation.

moment there is a strong focus on the Indo-Pacific region (UK2). The UK has a cyber capacity building budget of almost 22 million British Pound for the fiscal year 2021-2022 that is a mix of ODA and non-ODA (UK1), which is nearly 26 million EURO over a period of one year.

In sum, all four countries engage in cyber capacity building activities although their priorities regarding topics, recipients, and priorities vary due to their strategies, policies, but also their available budget. Nevertheless, all countries highlight that although they have their own ideas and priorities regarding cyber capacity building topics and activities, it does depend on what the recipient country wants. The next section will focus on what the twelve respondents identified as drivers for their cyber capacity building investments.

4.3.3 Drivers for cyber capacity building investments

The countries highlighted several different drivers that determine their investments in cyber capacity building activities, that can be captured under seven headings that are outlined below. First, the importance of the regional and/or historical ties with countries are a primary driver for multiple countries that is in line with their overall foreign policy priorities. Both Australia and Canada indicated that their priority region is their own region, implying respectively the Pacific and the Americas. The UK has a strong focus on the Commonwealth countries due to their historical ties (UK2).

Secondly, an important determining factor for Australia and the UK is all or part of their cyber capacity funds are labeled as ODA funding. As mentioned earlier in this study, this means that only countries with the ODA status are eligible to receive this funding. Therefore, Australia highlights this as their main 'discriminating' factor as part of their aid budget (AUS1). The UK has a mixed ODA/non-ODA cyber capacity budget and can be more flexible if they want to support countries that are not ODA eligible (UK1). The cyber capacity funding of Canada and the Netherlands is not linked to ODA funding. In the case of Canada, this is because their cyber capacity programs need to demonstrate how it support the Canadian security and interest (CAD3), which makes it not eligible for ODA.

A third driver that can be identified is related to security, and more specifically to threats. The UK conducts analyses from which countries threats are originated towards the UK. This does not imply that the country is purposefully supporting the threat, but rather that there is a weak link in the supply chain or just the lack of cyber capacity within that country (UK2). Therefore, improving that country's cybersecurity will also impact the UK's own security. This is similar to Australia that highlights the importance of the security incentive *"you're only as strong as your weakest link"* (AUS3).

Fourthly, requests from (potential) recipient countries directly or via country's Embassies also drive their cyber capacity building program. The Netherlands highlights that their Embassies have a key role in providing input on whether the Netherlands can support that specific country (NL1) and through these bilateral conversations more clarity is provided on the respective country's needs (NL2). The UK also underlines that their Embassies and High Commission Overseas are primarily responsible for facilitating the dialogue to gain a better understanding of a country's needs (UK1). Important to highlight here is that cyber capacity building is considered a two-way street (AUS2), or a two-way conversation (UK1) regarding the recipient's cyber capacity needs and how the donor can provide support.

The fifth driver is linked to the need of the donor countries to establish a network with points of contacts. The Netherlands and the UK pointed out that their counterparts, for example in a Ministry of Foreign Affairs that have cyber in their portfolio, do not exist in developing countries or LDCs (UK3). Therefore, cyber capacity building projects are also aimed to ensure that these structures and positions are established to interact and exchange knowledge and expertise, for example what their cyber capacity needs are or how they view cyberspace (NL3).

The sixth driver that almost all interview respondents highlighted is that they consider the status of countries, regarding for example human rights, before they engage in cyber capacity building activities. This is indirectly related to how recipient countries view the governance of the internet. If a more controlled internet by the state is preferred, and if the human rights situation in a country is questionable, then increased cyber capacity could lead to surveillance of minorities. Australia highlighted that human rights are considered as it can influence whether *"we won't provide certain technologies to that country or provide training on how to use certain technologies*" (AUS2). Canada stated that some cyber capacity building activities can have *"adverse human rights issues that can be oppressive in some cases"*, and therefore the country needs to be considered (CAD3). The Netherlands noted that they assess countries regarding human rights violations, but that this is standard in the appraisal of capacity building projects (NL2). The UK mentioned that they conduct assessments, if there are human rights violations, this can narrow the scope of the cyber capacity building activity; however, they will still engage with that country if they believe that *"some level of capacity building can still provide benefit*" (UK1).

The seventh driver, connected to the previous one, is that at least one ore multiple representatives of each of the four countries did mention that there is a focus on countries that are "like-minded", "on the fence", and/or that do not have the capabilities yet to have a clear position in the internet governance debate. Canada states that the selection for recipient countries related to projects linked to cyber diplomacy, they aim for more like-minded countries or the fence sitters (CAD2). The UK has a similar approach with similar cyber diplomacy projects, that they do not limit their selection to like-minded countries, but they would also consider countries that are on the fence or even those that tend to lean to the other camp (UK3).

In sum, there are multiple drivers for cyber capacity building investment that can be linked to a development, security, and foreign policy objective. Interestingly, the foreign policy objective is not just linked to the sixth and seventh driver, but especially the regional and historical ties that are linked to foreign policy objectives can have a significant impact on how countries determine their cyber capacity support. For the purpose of this study, the sixth and seventh drivers are most relevant as these can be linked to the internet governance debate and will therefore be explored more in-depth in the next sub-section.

4.3.4 Cyber capacity building, foreign policy objectives, and the internet governance debate

This sub-section will focus on whether the donor countries view that cyber capacity building investments are linked with foreign policy objectives, and if cyber capacity building investments can influence a recipient's stance in the internet governance debate. The Women in Cyber Fellowship project is included as an example, as it is a cyber capacity project that all four donors are involved in, and that can have a direct impact on UN voting.

First, countries were asked whether they think the assumption is true for their respective organization that cyber capacity building investments are linked to foreign policy objectives. Nearly all respondents answered that to a certain extent this is true. For example, a UK representative mentioned that a core objective is to be able to get people online whilst instilling values regarding an open, free, secure, and peaceful internet (UK3). However, it is not the only or the most prioritized driver. Foreign policy objectives go beyond political incentives; it includes, amongst others also security and development objectives, as emphasized in the literature review, but also other strategic priorities regarding regions or topics as gender. These foreign policy objectives trickle down to the decision-making process in cyber capacity building investments. Australia highlights that their foreign policy objectives in the Indo-Pacific are reflected in their cyber capacity program (AUS3). An additional argument brought forward by the Netherlands is that sometimes cyber capacity building can be used to have conversations with countries regarding certain ideas and values, since it is not as sensitive a topic as for example maritime security (NL2).

Secondly, the donor countries were also asked whether they think that cyber capacity building can influence a country's position in the internet governance debate. Multiple respondents argued that through cyber capacity building activities, countries are exposed to issues as the internet governance debates, and they can develop the capacities to reflect on these discussions and the different positions (AUS2). An Australian representative mentioned that cyber capacity building is *"just one tool in the diplomatic toolbox when it comes to influencing nations for a variety of reasons"* (AUS1). Representatives from the UK (UK2 & UK3), Canada (CAD1 & CAD2), and the Netherlands (NL1 & NL3) highlighted that in the long run, cyber capacity building can influence a country due to awareness raising, trainings, dialogues, and engagement that countries gain a better understanding that can have an effect eventually on their position in the internet governance debate. Another representative from the UK was more direct stating that *"I think it can, and I think it should"*, since cyber capacity building activities are rooted in certain values that can impact and influence a recipient country (UK1).

An example of a cyber capacity building investment that can directly impact the voting of UNGA resolutions on cyber-related issues is the Women in Cyber Fellowship project. This project, initiated by Australia, is a cyber diplomacy capacity project that all four donor counties have engaged in from the start (AUS2). All four countries highlighted the importance of this project due to the prioritization of gender and female representation in the field of cybersecurity. Canada refers to it as the *"feminist focus in its foreign policy"* (CAD1). The project already received outstanding results. In 2019, the coalition funded 35 fellows to the 2019 OEWG debate (CAD2). Due to the fellows' participation, it was the first time that gender parity was reached not only in the representatives, but also the interventions that were made (47%) – which was the first time in the UN First Committee on Disarmament and International Security, and about half of these interventions were made by fellows of this project (AUS2). Besides increasing the number of female representatives in the UN cyber debates, other motivations are to increase awareness on the issues as well as to increase their negotiation abilities. Through the project, trainings and network opportunities are offered to the fellows that also allow to gain a better and more in-depth understanding of the issues at hand. The UK also highlighted that with their fellow selection, they would not limit their selection to like-minded countries, but they would also consider countries that are on the fence or even those that tend to lean to the other camp (UK3).

However, most respondents did refer in their answer that countries' positions in the internet governance debate are also dependent on many other strategic and geopolitical factors. One respondent underlined that there can be differences of perspectives between capital and the representative at the UN and another argument is that sometimes countries choose to abstain due to geopolitical reasons (NL3). A representative from the Netherlands also posed a dilemma that some recipient countries face: what if an underdeveloped country is offered ICT infrastructure, even if that respective donor country does not comply with international law, would the recipient turn this down even though it is in dire need of infrastructure? (NL1). Therefore, it is essential if cyber capacity building is to make an impact on a country that the investment is long-term and sustainable.

In sum, cyber capacity building can be linked to foreign policy objectives. However, it is not limited to the political, nor the development and security objectives, it also includes broader strategic priorities as regional and historical ties or topics as gender. These foreign policy objectives trickle down to the decision-making process in cyber capacity building investments. Further, most respondents agree that cyber capacity building can influence a country's stance in the internet governance debate, as one respondent summarized it is one of the available tools that countries can use. However, the position of countries does depend on many other factors than cyber capacity building, such as strategic and geopolitical factors.

4.3.5 Future of cyber capacity building

All donor countries have been active in the young field of cyber capacity building for quite some years, the UK even since 2012; how do they see this field evolve? Multiple respondents see the field of cyber capacity building growing, with more stakeholders becoming involved, and professionalizing. One respondent reflected as the digital divide is growing, and technology is rapidly evolving, and cyber capacity building efforts will need to become more focused and efficient if they want to keep up (NL1). From each country one or multiple representatives also called for more coordination between donor countries on cyber capacity building investments. The downside of having more actors in the field of cyber capacity building is that recipient countries might not have the ability to absorb and effectively implement the cyber capacity support they receive. One of the Australian representatives highlighted that more donor countries are becoming active in the Pacific, but that Pacific Island representatives sometimes only have one or two people working on cyber, and they cannot handle the multiple offers for support (AUS2). Another element that two of the Canadian representatives highlighted was that the extension of the OEWG with five years and the Plan of Action can have quite large implications for cyber capacity building (CAD1 & CAD2). Moreover, as one interview respondent mentioned, cyber capacity building is a means to an end, the aim is that countries have developed eventually sufficient cyber maturity that cyber capacity building becomes obsolete (NL1). However, this end goal is far away, and many steps will need to be taken to get there.

4.3.6 Conclusion on motivation of countries on cyber capacity building investments

In conclusion, this section examined what the motivation of countries is to invest in cyber capacity building activities. As is demonstrated in the answers from the interview respondents, there is not one single and simple answer to this question. There are multiple reasons and variables linked to cyber capacity building investments. First, it depends on a donor country's priorities and the type of funding they have available, for example whether it is ODA-eligible. Secondly, target countries can be due to regional priorities, strategic and/or historical ties, security arguments due to potential threats, direct requests from recipients, local needs highlighted through cyber diplomats, and the position of a country in the internet governance debate. Thirdly, although most respondents agree that cyber capacity building is to some extent linked to a country's foreign policy objectives, this does not imply that these are political incentives. It has become distinctly clear that 'foreign policy objectives' is such a broad concept, that lots of incentives can be linked to it, including the security and development incentive, and many more.

5. Conclusion

The last chapter of this thesis will cover both the conclusion and recommendations for future research.

5.1 Conclusion

The aim of this study was to examine the drivers for donor countries to invest in international cyber capacity building activities and whether this is related to promoting their foreign policy objectives regarding the internet governance debate. Although the academic debate refers to a connection between cyber capacity building investments and foreign policy objectives, such as the internet governance debate, the empirical evidence is severely lacking. Therefore, this study aimed to build and expand the academic debate by analyzing whether internet governance divisions shape international cyber capacity building investment decisions. The hypothesis applied in this study was: *International capacity building investments are targeted at like-minded countries and digital swing states*. This thesis contributes to the academic debate through pioneering with empirical evidence linking cyber capacity building with the internet governance debate by using open-source databases, such as UN voting records and Cybil, and twelve semi-structured interviews with four donor countries from the "multi-stakeholder and open" internet group.

Overall, the analysis demonstrated that internet governance divisions are considered by donor countries regarding cyber capacity building investments. Multiple interview respondents indicated that, specifically with cyber diplomacy capacity projects, this is used as one of the indicators, and the hypothesis is accurate that the preference goes to like-minded countries and countries on the fence (digital swing states), and also occasionally countries that slightly tend to lean the other way. Nevertheless, both the interviews and the Cybil project data analysis demonstrate that it is only one of many drivers that are considered for determining cyber capacity investments.

For instance, the UN voting records demonstrated how countries have voted during the past five cyber-related UNGA resolutions to gain a better understanding where each country stands in the internet governance debate. Nine types of behavior could be identified across three categories: "multi-stakeholder and open", "sovereign and controlled", and "digital swing states". The first group has 56 countries, and the digital swing states 59, and these groups were used to examine more closely whether they are targeted for cyber capacity building activities by donor countries from the “multi-stakeholder and open” internet group. Although almost all of the countries in the digital swing states receive cyber capacity support from donor countries; the Cybil project data did not demonstrate a link to any particular category where there were multiple activities across those respective countries. Upon closer examination, it became evident that a connection could often be made if a donor country has a particular regional focus (its “own” region) or if there were any historical ties (e.g., Commonwealth). Similarly for the like-minded countries - excluding the donors - there was also not a link found to cyber capacity activities, most countries did not even receive any cyber capacity support. Arguments for this could be that those countries have a sufficient level of cybersecurity and/or they have their own available resources and are not dependent on development aid. All in all, the Cybil data did not provide any concrete evidence in support of the hypothesis.

In-depth interviews with representatives from the Ministry of Foreign Affairs from Australia, Canada, the Netherlands, and the United Kingdom provided more insights in their drivers for international cyber capacity building investment decisions. The interview respondents validated the insights provided through the Cybil analysis, that regional and/or historical ties with specific countries and regions are key drivers for their cyber capacity building investments as this is outlined their over foreign policy priorities. For Australia and the UK, ODA eligible countries are prioritized since (some of) their cyber capacity building budget is tied to ODA funding. Other identified drivers are threat assessments to determine from countries originate threats to the donor countries (unintentionally) are also used; direct requests from potential recipients (via the Embassies); and the need for donor countries to establish counterparts in developing countries and LDCs. The last two drivers that were mentioned are (indirectly) linked to the internet governance debate. For example, the status of country towards human rights can be a key criterion whether to engage or not. Additionally, in the case of cyber diplomacy capacity projects, such as the Women in Cyber Fellowship, donor countries did mention that they target like-minded countries, countries that are on the fence (same as digital swing states), and sometimes countries that slightly tend to lean the other way.

Nearly all respondents agreed that cyber capacity building can be used as a tool for foreign policy. However, this does not imply that the internet governance debate is considered a priority in the drivers for cyber capacity building investments. Rather, the analysis demonstrated how many drivers are embedded in the donor countries’ foreign policy objectives. Foreign policy objectives go beyond just (geo)political incentives; it includes, amongst others also security and development objectives, as emphasized in the literature review, but also other strategic priorities regarding regions or topics as gender. These foreign policy objectives trickle down to the decision-making process in cyber capacity building investments, and therefore foreign policy objectives have a large impact in determining cyber capacity efforts.

Furthermore, the respondents did agree that cyber capacity building can influence to some extent the internet governance debate. The values of an open, free, and secure internet are integrated in all cyber capacity building efforts, and therefore can indirectly influence how countries perceive governance of the internet issue. Nonetheless, this does not imply that a direct link can be made between cyber capacity building and the internet governance debate. Additionally, respondents mentioned that cyber capacity building is only one of the available diplomatic tools in the toolbox to affect countries.

In conclusion, the empirical findings in this study demonstrate that capacity building activities can be used as a foreign policy tool to further national interests. This was also demonstrated in the literature review on capacity building and how this form of development aid can be understood through the lens of soft power promotion as part of a country's diplomatic toolbox. However, the findings in this study demonstrate that the academic debate thus far has neglected to emphasize that cyber capacity building is just one of the many diplomatic tools available to influence a country. Additionally, the study's findings reveal that influencing a country's position in the internet governance debate, is never a sole or even a prioritized driver for cyber capacity building investment decisions. Moreover, this study demonstrates that although the development, security, and foreign policy objectives are important drivers that are considered by donor countries for cyber capacity building; more in-depth research is necessary to further explore how (cyber) capacity building is embedded in a country's foreign policy objectives and how this affects their investment decisions.

5.2 Recommendations

There are several recommendations for future research that can be made due to the delimitations of this study and its findings that are highlighted below. First, the study narrowed its scope to the donor countries in the "multi-stakeholder and open" internet group. It would be relevant to conduct a similar study regarding donor countries in the "sovereign and controlled" internet group, since countries as China do invest in cyber capacity building efforts through their Belt and Road Space Information Corridor and Digital Silk Road. It would be interesting to compare and contrast with the results of this study.

The second recommendation is to examine how cyber capacity building investments of international and regional organizations are linked to the internet governance debate. This study excluded these activities, since it is not clear which countries are responsible for the investments, and how the decision-making of these international and regional organizations is guided. Since, with the exception of the EU and OECD, countries with different (or no established) ideologies on the internet are part of these organizations. However, this could provide new insights on how internet governance positions are influenced.

A third recommendation is connected to a follow-up of this study to examine the like-minded and digital swing states that received above-average cyber capacity building support more closely, focusing on the actual cyber capacity investments received per country. This information is not transparent and publicly available, but could provide interesting insights regarding potential return of investment questions.

Fourthly, an interesting finding of this study was that Australia and the UK can link their cyber capacity investments to ODA while Canada and the Netherlands cannot. Therefore, it would be relevant to examine how ODA funding can be used for cyber capacity investments since this would entail more resources becoming available for cyber capacity building.

Lastly, as recommended in the conclusion, further research is necessary to explore how cyber capacity building is embedded within the foreign policy objectives of countries, how this impacts other drivers for cyber capacity building, and how this can provide advantages and limitations to cyber capacity investment decisions.

6. References

Ahmed, Jesmine. "The Theoretical Significance of Foreign Policy in International Relatons: An Analysis" 7, no. 2 (2020): 787–92.

Baxter, Pamela, and Susan Jack. "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers." *The Qualitative Report* 13, no. 4 (December 1, 2008): 544–59. https://doi.org/10.46743/2160-3715/2008.1573.

Bossey, Château De. "Report of the Working Group on Internet Governance," 2005.

Broeders, Dennis, and Bibi van den Berg. "Governing Cyberspace Behavior, Power, and Diplomacy." edited by Dennis Broeders and Bibi van den Berg. Rowman & Littlefield, 2020.

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 (2020): 917–38. https://doi.org/10.1080/01436597.2020.1729729.

Capacity Development Group, UNDP. "Overview of UNDP's Approach to Supporting Capacity Development," no. August (2009).

Chandler, David. *International Statebuilding: The Rise of Post-Liberal Governance*. London: Routledge, 2010.

Clements, Kevin P., Volker Boege, Anne Brown, Wendy Foley, and Anna Nolan. "State Building Reconsidered: The Role of Hybridity in the Formation of Political Order." *Http://Dx.Doi.Org/10.1177/003231870705900106* 59, no. 1 (2017): 45–56. https://doi.org/10.1177/003231870705900106.

Collett, Robert. "Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures." *Journal of Cyber Policy*, 2021. https://doi.org/10.1080/23738871.2021.1948582.

Collett, Robert, and Nayia Barmpaliou. "International Cyber Capacity Building: Global Trends and Scenarios," 2021. https://doi.org/10.2815/06590.

Creese, Sadie, William H. Dutton, and Patricia Esteve-González. "The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions." *Personal and Ubiquitous Computing*, 2021. https://doi.org/10.1007/s00779-021-01569-6.

"Cybercrime To Cost The World $10.5 Trillion Annually By 2025." Accessed October 17, 2021. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

"Cybil Portal." Accessed August 30, 2021. https://cybilportal.org/projects/.

"Cybil Portal - Estonia Projects." Accessed November 20, 2021. https://cybilportal.org/projects/?_sfm_funders_relationship=2844-%2C-765.

Dahl, Robert A. "The Concept of Power." *Behavioral Science* 2, no. 3 (1957). https://fbaum.unc.edu/teaching/articles/Dahl_Power_1957.pdf.

DeJonckheere, Melissa, and Lisa M Vaughn. "Semistructured Interviewing in Primary Care Research: A Balance of Relationship and Rigour." *Family Medicine and Community Health* 7, no. 2 (March 1, 2019): e000057. https://doi.org/10.1136/FMCH-2018-000057.

Denardis, Laura, and Mark Raymond. "Thinking Clearly about Multistakeholder Internet Governance," 2013.

Department of Foreign Affairs and Trade. *Australia's International Cyber and Critical Tech Engagement Strategy*. *Australian Government Department of Foreign Affairs and Trade*, 2021. https://www.internationalcybertech.gov.au/.

Desforges, Alix. "Representations of the Cyberspace: A Geopolitical Tool." *Herodote*, no. 152–153 (2014): 67–81. https://doi.org/10.3917/her.152.0067.

Digital Watch Observatory. "UN GGE and OEWG." Accessed February 26, 2021. https://dig.watch/processes/un-gge.

Dolan, Jonathan. "Digital Inclusion and a Trusted Internet: The Role of the International Development Community in Balancing Internet Access and Cybersecurity." *DAI*, no. October (2018).

Donais, Timothy. "Inclusion or Exclusion? Local Ownership and Security Sector Reform." *Studies in Social Justice* 3, no. 1 (2009): 117–31. https://doi.org/10.26522/ssj.v3i1.1027.

Dutton, William H, Sadie Creese, Ruth Shillair, and Maria Bada. "Cybersecurity Capacity." *Journal of Information Policy* 9, no. May 2021 (2019): 280–306.

Edmunds, Timothy, and Ana Juncos. "Constructing the Capable State: Contested Discourses and Practices in EU Capacity Building." *Cooperation and Conflict* 55, no. 1 (2020): 3–21.

Ferguson, Niall. *Colossus: The Price of America's Empire*. New York: Penguin Press, 2004.

Gray, Collin S. "Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century," 2011.

Gustafsson, Johanna. "Single Case Studies vs. Multiple Case Studies: A Comparative Study," 2017. https://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf.

Hameiri, Shahar. "Capacity and Its Fallacies: International State Building as State Transformation." *Millennium: Journal of International Studies* 38, no. 1 (2009): 55–81. https://doi.org/10.1177/0305829809335942.

Hathaway, Melissa, and Francesca Spidalieri. “Integrating Cyber Capacity into the Digital Development Agenda,” 2021. www.digitaldevelopmentpartnership.org.

Hohmann, Mirko, Alexander Pirang, Thorsten Benner, Maria Bada, Belisario Contreras, Rahel Dette, Julian Lehmann, et al. “Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach.” *Global Public Policy Institute (GPPi)*, 2017. http://www.gppi.net/fileadmin/user_upload/media/pub/2017/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf.

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

International Telecommunication Union. *Global Cybersecurity Index*, 2020.

Internet Society (ISOC). “A Policy Framework for an Open and Trusted Internet: An Approach for Reinforcing Trust in an Open Environment,” 2017.

Jick, Todd D. “Mixing Qualitative and Quantitative Methods: Triangulation in Action.” *Administrative Science Quarterly* 24, no. 4 (1979): 602. https://doi.org/10.2307/2392366.

Kaldor, Mary, Mary Martin, and Sabine Selchow. “Human Security: A New Strategic Narrative for Europe.” *International Affairs* 83, no. 2 (2007): 273–88. https://doi.org/10.1111/j.1468-2346.2007.00618.x.

Kleinwächter, Wolfgang. “Framing the Internet Governance Debate: The Long Road to WSIS+20 (2025).” *CircleID*, March 4, 2021. https://circleid.com/posts/20210304-framing-the-internet-governance-debate-long-road-to-wsis-2025/.

Klimburg, Alexander, and Louk Faesen. “A Balance of Power in Cyberspace.” In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi Van den Berg, 145–71. London: Rowman & Littlefield, 2020. https://www.researchgate.net/profile/Dennis-Broeders-2/publication/343833386_Governing_Cyberspace_Behavior_Power_and_Diplomacy/links/5f43c484a6fdcccc43f584f0/Governing-Cyberspace-Behavior-Power-and-Diplomacy.pdf#page=154.

Klimburg, Alexander, and Hugo Zylberberg. “Cyber Security Capacity Building: Developing Access,” no. 6 (2015).

Kühl, Stefan. “Capacity Development as the Model for Development Aid Organizations.” *Development and Change* 40, no. 3 (2009): 551–77. https://doi.org/10.1111/j.1467-7660.2009.01538.x.

Kurbalija, Jovan. *An Introduction to Internet Governance*. 7th ed. Geneva: DiploFoundation. Accessed October 28, 2021. https://wp4.diplomacy.edu/sites/default/files/AnIntroductiontoIG_7th edition.pdf.

"List of OECD Member Countries ." Accessed December 4, 2021. https://www.oecd.org/about/document/ratification-oecd-convention.htm.

"Methodological Triangulation in Qualitative Research In: Doing Triangulation and Mixed Methods," 2018. https://doi.org/10.4135/9781529716634.

Morar, David. "Perspectives on Internet Governance: (Why) Does Internet Governance Matter?," 2016.

Morgenthau, Hans. "The Political Theory of Foreign Aid Related Papers," 1965.

Morgus, Robert. "Securing Digital Dividends Mainstreaming Cybersecurity in International Development," 2018.

Morgus, Robert, Jocelyn Woolbright, and Justin Sherman. "The Digital Deciders," 2018. https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

"MOU Between Papua New Guinea and Australia Relating to Cyber Security Cooperation | Australian Government Department of Foreign Affairs and Trade." Accessed November 20, 2021. https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/mou-between-papua-new-guinea-and-australia-relating-to-cyber-security-cooperation.

Muller, Lilly Pijnenburg. "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities." *Norwegian Institute of International Affairs*, no. 3 (2015): 23. https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf.

New America. "The Digital Deciders - Mapping Tool," 2018. https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/understanding-the-clusters-through-data/.

Nye, Joseph. "The Future of Power." London, May 10, 2011. https://www.chathamhouse.org/sites/default/files/public/Meetings/Meeting Transcripts/100511nye.pdf.

Nye, Joseph Jr. *Soft Power: The Means To Success In World Politics*. *Helvetica Chimica Acta*. PublicAffairs, 2005.

Nye, Joseph Jr. *Soft Power: The Means to Success in World Politics*. New York Public Affairs, 2004.

Nye, Joseph S. "The Regime Complex for Managing Global Cyber Activities." *Global*

Commission on Internet Governance. Vol. 1, 2014. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Ociepka, Beata. “Dyplomacja Publiczna.” *Wydawnictwo Uniwersytetu Wrocławskiego*, 2008.

OECD. “Official Development Assistance (ODA) What Is ODA?,” 2019. www.oecd.org/dac.

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

———. “Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development.” *Issue* 21, no. December (2014). https://doi.org/10.2815/43313.

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

“Principles | Principles for Digital Development.” Accessed October 3, 2021. https://digitalprinciples.org/principles/.

Rolland, Nadege, Mathieu Duchâtel, Kristen Gunness, Guifang Xue, Dirk van der Kley, Michael S Chase, Raffaello Pantucci, and Alessandro Arduino. “Securing the Belt and Road Initiative: China’s Evolving Military Engagement Along the Silk Roads,” n.d.

Rosenau, James N. “Governance in the Twenty-First Century.” *Source: Global Governance* 1, no. 1 (1995): 13–43.

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

Schia, Niels Nagelhus, and Johann Ole Willers. “Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries,” no. February (2021): 221–30. https://doi.org/10.1007/978-3-319-95873-6_115.

Scholte, Jan Aart. “Polycentrism and Democracy in Internet Governance,” no. 165 (2017): 165–84.

Shenton, Andrew K. “Strategies for Ensuring Trustworthiness in Qualitative Research Projects.” *Education for Information* 22, no. 2 (2004): 63–75. https://doi.org/10.3233/EFI-2004-22201.

Sherman, Justin, and Robert Morgus. “Breaking Down the Vote on Russia’s New Cybercrime Resolution at the UN.” *New America*, 2018. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/breaking-down-vote-russias-new-cybercrime-resolution-un/.

Snow, Nancy. *Routledge Handbook of Public Diplomacy* , 2020. https://doi.org/10.4324/9780429465543.

Stoker, Gerry. “Governance as Theory: Five Propositions.” *International Social Science Journal* 68, no. 227–228 (March 1, 2018): 15–24. https://doi.org/10.1111/ISSJ.12189.

Strickling, Lawrence E, and Jonah Force Hill. “Multi-Stakeholder Internet Governance : Successes and Opportunities.” *Journal of Cyber Policy* 2, no. 3 (2017): 296–317. https://doi.org/10.1080/23738871.2017.1404619.

The World Bank Group. *Digital Dividends*, 2016.

“UN General Assembly: Voting Records Search.” Accessed November 20, 2021. https://www.un.org/en/ga/documents/voting.asp.

United Nations. “Transforming Our World: The 2030 Agenda for Sustainable Development,” 2015.

United Nations Development Programma (UNDP). “Capacity Development: A UNDP Primer,” 2009.

United Nations General Assembly. “UNGA Resolution A/RES/73/187: Countering the Use of Information and Communications Technologies for Criminal Purposes.” UN, January 14, 2019. https://digitallibrary.un.org/record/1660536.

———. “UNGA Resolution A/RES/73/266: Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.” UN, January 2, 2019. https://digitallibrary.un.org/record/1658328.

———. “UNGA Resolution A/RES/73/27: Developments in the Field of Information and Telecommunications in the Context of International Security.” UN, December 11, 2018. https://digitallibrary.un.org/record/1655670.

———. “UNGA Resolution A/RES/74/247: Countering the Use of Information and Communications Technologies for Criminal Purposes.” UN, January 20, 2020. https://digitallibrary.un.org/record/3847855.

———. “UNGA Resolution A/RES/75/240: Developments in the Field of Information and Telecommunications in the Context of International Security.” UN, January 4, 2021. https://digitallibrary.un.org/record/3896458.

———. “United Nations General Assembly Consensus Report GGE 2015: A/70/174,” 2015. https://undocs.org/A/70/174.

Vallejo, Bertha, and Uta Wehn. “Capacity Development Evaluation: The Challenge of the Results Agenda and Measuring Return on Investment in the Global South.” *World Development* 79 (2016): 1–13. https://doi.org/10.1016/j.worlddev.2015.10.044.

Wijninga, Peter, Willem Theo Oosterveld, Jan Hendrik Galdiga, and Philipp Marten. “4 State and Non-State Actors: Beyond the Dichotomy.” In *Strategic Monitor 2014: Four*

Strategic Challenges, edited by Joris Van Esch, Frank Bekkers, Stephan De Spiegeleire, Tim Sweijs, Eline Chivot, Jan Hendrik Galdiga, Maarten Gehem, et al., 141–62, 2014. https://www.jstor.org/stable/pdf/resrep12608.8.pdf?refreqid=excelsior%3A4a4f2bf59c47e305ab35931ed0c7ceb7.

Willers, Johann Ole. "Seeding the Cloud: Consultancy Services in the Nascent Field of Cyber Capacity Building." *Public Administration*, 2021. https://doi.org/10.1111/PADM.12773.

"Women in Cyber Fellowship - Cybil Portal." Accessed November 4, 2021. https://cybilportal.org/projects/women-in-cyber-fellowship/.

Yin, R.K. *Case Study Research: Design and Methods*. 4th ed. Thousand Oaks, CA: Sage Publications, 2009.

Zielinska, Karolina. "Development Diplomacy. Development Aid as a Part of Public Diplomacy in the Pursuit of Foreign Policy Aims: Theoretical and Practical Considerations." *Historia i Polityka* 16, no. 16 (2016): 9–26.

ANNEX 1: Overview of UNGA votes per country

Countries	**A/RES/73/27**	**A/RES/73/266**	**A/RES/73/187**	**A/RES/74/247**	**A/RES/75/240**
Afghanistan	Y	Y	V	V	Y
Albania	N	Y	N	N	N
Algeria	Y	A	Y	Y	Y
Andorra	N	Y	N	N	N
Angola	Y	V	Y	V	A
Antigua and Barbuda	A	V	A	Y	V
Argentina	Y	Y	A	A	Y
Armenia	Y	Y	Y	Y	Y
Australia	N	Y	N	N	N
Austria	N	Y	N	N	N
Azerbaijan	Y	Y	Y	Y	Y
Bahamas	A	Y	A	A	A
Bahrain	Y	Y	Y	A	Y
Bangladesh	Y	Y	A	A	Y
Barbados	Y	Y	A	A	A
Belarus	Y	A	Y	Y	Y
Belgium	N	Y	N	N	N
Belize	Y	Y	Y	N	A
Benin	V	Y	Y	V	V
Bhutan	Y	Y	Y	Y	Y
Bolivia	Y	N	Y	A	Y
Bosnia and Herzegovina	Y	Y	N	N	Y
Botswana	A	A	Y	Y	Y
Brazil	A	Y	Y	A	A
Brunei Darussalem	Y	Y	Y	Y	Y
Bulgaria	N	Y	N	N	N
Burkina Faso	Y	Y	Y	V	V
Burundi	Y	V	Y	Y	Y
Cabo Verde	Y	V	A	N	A
Cambodia	Y	A	Y	Y	Y
Cameroon	V	A	Y	Y	V
Canada	N	Y	N	N	N
Central African Republic	Y	V	V	Y	V
Chad	V	V	Y	Y	Y
Chile	A	Y	N	N	N
China	Y	N	Y	Y	Y
Colombia	Y	Y	A	N	N
Comoros	Y	N	V	V	V
Congo	Y	V	Y	V	V
Costa Rica	Y	Y	A	A	Y

Côte D'Ivoire	Y	A	Y	A	Y
Croatia	N	Y	N	N	N
Cuba	Y	N	Y	Y	Y
Cyprus	N	Y	N	N	N
Czech Republic	N	Y	N	N	N
North-Korea	Y	N	Y	Y	Y
Dem. Republic of Congo	Y	V	A	V	V
Denmark	N	Y	N	N	N
Djibouti	Y	Y	A	A	Y
Dominica	V	V	Y	V	V
Dominican Republic	Y	Y	N	N	Y
Ecuador	Y	Y	Y	A	Y
Egypt	Y	N	Y	Y	Y
El Salvador	Y	Y	Y	A	Y
Equatorial Guinea	Y	A	Y	Y	Y
Eritrea	Y	Y	Y	Y	Y
Estonia	N	Y	N	N	N
Eswatini	A	V	V	V	V
Ethiopia	Y	Y	Y	Y	Y
Fiji	A	Y	A	V	A
Finland	N	Y	N	N	N
France	N	Y	N	N	N
Gabon	V	V	Y	Y	Y
Gambia (The)	Y	V	A	Y	Y
Georgia	N	Y	N	N	N
Germany	N	Y	N	N	N
Ghana	Y	Y	A	A	V
Greece	N	Y	N	N	N
Grenada	Y	Y	A	V	V
Guatemala	Y	Y	A	A	A
Guinea	Y	Y	Y	Y	V
Guinea Bissau	Y	V	Y	V	V
Guyana	Y	Y	A	A	A
Haiti	A	Y	A	A	V
Honduras	Y	Y	N	N	Y
Hungary	N	Y	N	N	N
Iceland	N	Y	N	N	N
India	Y	Y	Y	Y	A
Indonesia	Y	Y	Y	Y	Y
Iran	Y	N	Y	Y	Y
Iraq	Y	Y	Y	Y	Y
Ireland	N	Y	N	N	N
Israel	N	Y	N	N	N

Italy	N	Y	N	N	N
Jamaica	Y	Y	Y	Y	Y
Japan	N	Y	N	N	N
Jordan	Y	Y	Y	Y	Y
Kazakhstan	Y	Y	Y	Y	Y
Kenya	Y	Y	Y	Y	Y
Kiribati	V	V	N	V	Y
Kuwait	Y	Y	Y	Y	Y
Kyrgyzstan	Y	V	Y	Y	Y
Laos	Y	A	Y	Y	Y
Latvia	N	Y	N	N	N
Lebanon	Y	Y	Y	Y	Y
Lesotho	Y	Y	A	A	Y
Liberia	Y	Y	A	V	V
Libya	Y	Y	Y	Y	A
Liechtenstein	N	Y	N	N	N
Lithuania	N	Y	N	N	N
Luxembourg	N	Y	N	N	N
Madagascar	Y	Y	Y	Y	Y
Malawi	Y	A	Y	Y	A
Malaysia	Y	Y	Y	Y	Y
Maldives	Y	Y	Y	Y	Y
Mali	Y	Y	Y	Y	A
Malta	N	Y	N	N	N
Marshall Islands	N	Y	N	N	V
Mauritania	Y	Y	Y	Y	Y
Mauritius	Y	Y	A	A	Y
Mexico	Y	Y	A	A	Y
Micronesia	V	Y	N	N	V
Monaco	N	Y	N	N	N
Mongolia	Y	Y	Y	Y	Y
Montenegro	N	Y	N	N	N
Morocco	Y	Y	Y	A	Y
Mozambique	Y	A	Y	Y	Y
Myanmar	Y	A	Y	Y	Y
Namibia	Y	A	Y	Y	Y
Nauru	V	V	A	Y	V
Nepal	Y	Y	Y	Y	Y
Netherlands	N	Y	N	N	N
New Zealand	N	Y	N	N	N
Nicaragua	Y	N	Y	Y	Y
Niger	Y	V	Y	Y	A
Nigeria	Y	Y	Y	Y	A

North Macedonia	N	Y	N	N	N
Norway	N	Y	N	N	N
Oman	Y	Y	Y	Y	Y
Pakistan	Y	A	Y	Y	Y
Palau	Y	A	Y	A	A
Panama	Y	Y	N	N	Y
Papua New Guinea	A	A	A	A	A
Paraguay	Y	Y	A	N	Y
Peru	Y	Y	A	A	Y
Philippines	Y	Y	A	A	Y
Poland	N	Y	N	N	N
Portugal	N	Y	N	N	N
Qatar	Y	Y	Y	Y	Y
Republic of Korea	A	Y	N	N	N
Republic of Moldova	A	Y	N	N	N
Romania	N	Y	N	N	N
Russian Federation	Y	N	Y	Y	Y
Rwanda	A	V	A	Y	Y
Saint Kitts and Nevis	V	Y	Y	Y	V
Saint Lucia	Y	Y	Y	Y	Y
Saint Vincent	Y	Y	Y	Y	Y
Samoa	Y	V	A	V	Y
San Marino	N	Y	N	N	N
Sao Tome and Principe	Y	Y	Y	V	V
Saudi Arabia	Y	Y	Y	A	Y
Senegal	V	A	A	Y	Y
Serbia	Y	Y	Y	Y	Y
Seychelles	Y	V	Y	V	V
Sierra Leone	Y	Y	V	V	V
Singapore	Y	Y	Y	Y	Y
Slovakia	N	Y	N	N	N
Slovenia	N	Y	N	N	N
Solomon Islands	V	Y	N	A	A
Somalia	V	Y	Y	V	V
South Africa	Y	Y	Y	Y	Y
South Sudan	Y	V	Y	V	V
Spain	N	Y	N	N	N
Sri Lanka	Y	Y	Y	Y	Y
Sudan	Y	Y	Y	Y	Y
Suriname	Y	V	Y	Y	Y
Sweden	N	Y	N	N	N
Switzerland	A	Y	N	N	A
Syrian Arab Republic	Y	N	Y	Y	Y

Tajikistan	Y	Y	Y	Y	Y
Thailand	Y	Y	Y	Y	Y
Timor-Leste	Y	Y	A	A	Y
Togo	Y	Y	Y	Y	Y
Tonga	V	V	N	N	Y
Trinidad and Tobago	Y	Y	V	A	A
Tunisia	Y	Y	V	A	Y
Turkey	A	Y	A	A	N
Turkmenistan	Y	V	Y	Y	V
Tuvalu	Y	V	A	A	V
Uganda	Y	V	Y	Y	Y
Ukraine	N	Y	N	N	N
United Arab Emirates	Y	Y	Y	Y	Y
United Kingdom	N	Y	N	N	N
Tanzania	Y	Y	Y	Y	V
USA	N	Y	N	N	N
Uruguay	Y	Y	A	A	A
Uzbekistan	V	Y	Y	Y	Y
Vanuatu	Y	Y	N	V	V
Venezuela	Y	N	Y	Y	Y
Viet Nam	Y	Y	Y	Y	Y
Yemen	Y	Y	Y	Y	Y
Zambia	Y	V	Y	A	V
Zimbabwe	Y	N	Y	Y	Y

Voting summary	**Y: 119**	**Y: 138**	**Y: 94**	**Y: 79**	**Y: 92**
	N: 46	**N: 12**	**N: 59**	**N: 60**	**N: 50**
	A: 14	**A: 16**	**A: 33**	**A: 33**	**A: 21**
	V: 14	**V: 27**	**V: 7**	**V: 21**	**V: 30**

ANNEX 2: Interview Guide

Email to potential interview respondents
Subject: Invitation to participate in dissertation interview

Dear <name>,

As you are aware, I am the Program Coordinator at the Global Forum on Cyber Expertise (GFCE) Secretariat in The Hague. This time I am writing to you in my personal capacity.

After obtaining my MSc in Crisis and Security Management in 2016, I am now drafting my dissertation in pursuit of an Advanced MSc in Cyber Security at the University of Leiden. I am currently conducting interviews to obtain different views and perspectives and I would like to kindly ask for your participation. Please note that this study is being conducted independently from my professional career and does not in any way reflect the GFCE's outlook or opinion.

The dissertation will explore what the different motivations are for countries to invest in cyber capacity building (CCB) activities. Current academic literature focuses mainly on the political driver for cyber capacity building investments, for instance linking foreign policy objectives to the internet governance debate. My dissertation aims to deepen and to expand the academic discussion by exploring political as well as other motivations for countries to invest in cyber capacity building.

Therefore, I am looking to set up short interviews with three representatives within the same Ministry or Agency involved in cyber capacity building.

Given the <name organization>'s significant contributions to cyber capacity building, I would be very appreciative to talk to you and your colleagues, who are involved in different aspects of cyber capacity building. Preferably to someone involved in the UN negotiations or other international processes, someone responsible for CCB activities, and someone involved in specific CCB projects, for example the Women in Cyber Fellowship project.

Please let me know if you and your colleagues are willing to participate in a short interview of approximately 30 minutes in the coming weeks depending on your availability.

Looking forward to hearing from you.

Kind regards,
Manon van Tienhoven

Introduction to interview + Confidentiality
Thank you for agreeing to be a respondent for my dissertation for the Advanced MSc in Cyber Security. The aim of this study is to add and to expand the academic debate on the foreign policy objectives of donor countries related to cyber capacity building. Therefore, I am conducting interviews with representatives from donor countries in cyber capacity building activities to get a better understanding on how they perceive cyber capacity building in relation to their foreign policy objectives.

Your answers during this interview will remain confidential and will only be reviewed by myself and the two thesis supervisors: Dr. James Shires and Dr. Els de Busser. Your identity will also be withheld in the final documentation. If you do not feel comfortable answering any question, we can skip them. You are free to stop the interview at any point.

After hearing all this, are you comfortable to proceed with the interview?
[get explicit consent]

Are you okay with me recording the interview for transcript purposes?
[get explicit consent]

[start recording]

Interview questions

1. What is your understanding of cyber capacity building?
    a. Are you or have you been involved in cyber capacity building your organization?
2. Where does <name organization> stand in the ongoing internet governance debate?
3. Does your government engage in cyber capacity building activities?
    a. If yes, how do you select the cyber capacity building topics and activities to engage in?
    b. Are there criteria that potential recipients need to meet to receive your cyber capacity building support?
        i. How do you select your target countries for cyber capacity building activities?
        ii. Could you tell me something about your available budget for cyber capacity building?
        iii. Is it related to ODA funding?
4. There is an assumption that cyber capacity building activities are linked to country's foreign policy objectives. Do you think this is true for <name organization>?
    a. If yes, could you please elaborate how these activities are linked to a country's foreign policy objectives?
    b. If no, would you say that cyber capacity building is linked to other national objectives?
5. <Name organization> is involved in many cyber capacity building activities, for example the Women in Cyber Fellowship project, which aims to provide access and training to women diplomats from various regions, supporting their participation in the various UN processes. Why is it important for <name organization> to support this project?
    a. What do you foresee the recipients of this project to gain from this project?
6. According to the projects available on Cybil, <name organization> mainly supports cyber capacity building efforts in the <specify region(s)>. What is the reason for this?
7. Do you think cyber capacity building activities influence a recipient's stance in the internet governance debate?
8. How do you see cyber capacity building activities evolve in the future?

Conclusion

This brings us to the final part of the interview. Thank you for taking the time to do this interview with me. Upon completion of my dissertation, I can send you a copy. If you have any questions at a later time, please do not hesitate to contact me.