CYBER CAPACITY-BUILDING AS A GEOPOLITICAL TOOL:
THE GLOBAL NORTH AND GLOBAL SOUTH RELATIONS IN CONTEMPORARY CYBER DIPLOMACY

Anna Urbanovics
assistant professor
Ludovika University of Public Service, Department of Cybersecurity and e-Government
ORCID 0000-0003-2163-7273

Doi: 10.15170/PSK.2026.SI.01.02
Received: November 15, 2025
Accepted: April 16, 2026
Published: April 26, 2026

Citation:
Urbanovics, Anna (2026). Cyber Capacity-Building as a Geopolitical Tool: The Global North and Global South Relations in Contemporary Cyber Diplomacy. *Polarities*, 7(SI), 17–35.

Acknowledgements:
–

Abstract

Cyber diplomacy has become an important field, and one of the most efficient tools used by countries is cyber capacity building. This paper analyses these activities from the perspective of three key cyber diplomacy actors, the United Nations, the European Union, and the United States. As they follow different governance frameworks for cyber capacity building, the collaboration networks and regional focus of the projects they are involved in differ. This study uses a mixed methodology, combining descriptive statistics and network analysis. The analysis takes a data-oriented approach and data was gathered from the Cybil Portal. The results demonstrate that the United Nations has the most comprehensive network in terms of regional breakdown. The United States follows a great power logic, focusing on strategic regions. Meanwhile, the European Union is predominantly active in its neighborhood and plays an active role in promoting norms in these regions by its cyber capacity building engagements.

Keywords: *cyber diplomacy; cyber capacity-building; Cybil Portal; digital geopolitics; network analysis*

Introduction

Cybersecurity capacity-building has become a central instrument of international cooperation in cyberspace over the past two decades. It is defined as the "support and assistance aiming at empowering individuals, communities and governments to reduce risks stemming from access and use of information and communication technologies" (Homburger 2019). Policy actors have increasingly converged around the idea that capacity-building should enable states and societies to benefit from digitalization while mitigating the vulnerabilities associated with it. An EU Institute for Security Studies seminar report, for example, emphasized that cyber capacity-building should leave recipient countries better equipped to enjoy the economic and social benefits of cyberspace (European Commission, 2013). At the same time,

cybersecurity capacity-building has become a rapidly expanding field of practice, involving governments, international organizations, development agencies, technical communities, private companies, and civil society actors.

Cyber capacity building as a concept lies within the broader aspects of capacity building, which emerged in public administration debates in the 1950s, and was later studied within development studies. In this sense, capacity building referred to supporting states and societies in developing institutions, skills, and organizational frameworks to sustain long-term development processes (United Nations, 2002). Within development studies, the concept has always been contested, criticized both for its conceptual vagueness and for the power relations embedded in donor–beneficiary frameworks (Connelly, 2007; Wilén, 2009). Cybersecurity capacity-building inherits many of these tensions. Early definitions considered it as assistance from developed to developing countries aimed at enabling safe access to and use of digital technologies.

At the same time, cybersecurity capacity-building cannot be reduced to a development tool only. As digital infrastructures have become integral to economic systems, public administration, political processes, and national security, cybersecurity has emerged as a cross-cutting policy domain that links development, security, justice, foreign policy, and governance. The UN Group of Governmental Experts (GGE) in 2015, and later the Open-Ended Working Group (OEWG), explicitly connected capacity-building to international peace and security, calling on states to assist one another in improving the secure use of ICTs. In this context, cyber capacity-building has increasingly been framed as a form of international cooperation that contributes to cyber stability, confidence-building, and the diffusion of norms of responsible state behavior.

This paper aims to analyze cyber capacity building activities not as a technical assistant, but rather a geopolitical and a relational phenomenon within the emerging role of cyber diplomacy. This study does not measure the effectiveness of cyber capacity building instead; it focuses on the collaboration network of participating actors based on statistical data gathered from Cybil Portal database. The analysis points out the different approaches of main donor actors, namely the United Nations, the United States and the European Union. By mapping their networks, we gain insights on their institutional positions and different ways of international engagement – multilateral norm promotion, strategic security policy and regulatory external governance. Comparing their cyber capacity-building networks makes it possible to explore how different diplomatic logics are translated into concrete partnerships and projects.

By situating cyber capacity-building at the intersection of development, security, and governance, and by analyzing it as a networked field of practice, the article seeks to contribute to cyber diplomacy scholarship in two ways. First, it provides an empirical mapping of cyber capacity-building as an emerging domain of international

cooperation. Second, it advances a conceptual argument that cyber capacity-building should be understood as a modality of cyber diplomacy through which power is exercised, norms are diffused, and cyber order is constructed.

Despite a growing international literature on cyberdiplomacy, less attention has been paid to its role as a relational instrument through which geopolitical influence is exercised via structured collaboration networks. In particular, there is a lack of empirical, comparative analyses that connect theoretical insights on network power, norm diffusion, and geopolitical competition to observable patterns of cyber capacity-building partnerships. This article addresses this gap by conceptualizing cyber capacity-building as a form of competitive strategic alignment, through which donors seek to shape institutional environments, diffuse norms, and position themselves within global cyber governance networks.

The analysis is guided by the following research questions:

RQ1: How are cyber capacity-building networks structured across major donor actors (UN, US, EU)?

RQ2: What differences can be observed in their patterns of collaboration and regional engagement?

RQ3: To what extent do these patterns reflect distinct geopolitical strategies and forms of power in cyber diplomacy?

Building on the literature on network power and weaponized interdependence, the article expects that: multilateral actors (UN) will display more globally inclusive and decentralized networks; great powers (US) will exhibit selective, strategically concentrated engagement; regulatory actors (EU) will demonstrate regionally embedded and norm-driven network structures.

Cyberdiplomacy and cyber capacity building

The cyber domain has become one of the main domains of military operations in the last two decades, with its ever-growing number of cyber attacks (Urbanovics, 2023). In 2016, NATO recognized it as a domain of military operations and since then international actors have become active in the field. Building a comprehensive cyber policy requires "cybersecurity governance" referring to "a holistic and integrated vision of the security of networks, systems, services, and infra-structures in society. It includes the institutions, initiatives, policies, programs, and other mechanisms (formal and informal) that are part of an ecosystem of distributed capacities and responsibilities regarding cybersecurity" (Hurel, 2021). It is important to note that cyberdiplomacy has become a new field of power competition where state and

non-state actors equally compete for norm setting, strategic positions and network dominance (Carver, 2025).

The literature on capacity building assistance for digital development increasingly recognizes that these programs are not merely technical or development policy tools, but can also have strategic foreign policy significance (Hathaway& Spidalieri, 2021). The strategic dimension of such assistance can be interpreted in a donor-recipient relationship where a state donor provides assistance for digital development abroad (Seidl, 2024). They separate "digital" and "cyber" capacity building, even though there is a growing need for their integration in policy practice and diplomacy.

Reflecting these diverse origins, literature offers no single definition of cybersecurity capacity-building. Instead, existing definitions can be grouped into several clusters.

1. Development oriented: framing cyber capacity-building as support to developing countries to increase access to, and benefits from cyberspace.
2. Risk reduction: defining capacity-building as empowering individuals, communities, and governments to achieve their developmental goals by reducing digital security risks.
3. Complex activity: cyber capacity building as an umbrella activity, ranging from human resources development to institutional reform that safeguards the secure and open use of cyberspace (Pawlak 2014; Müller 2015).
4. Governance oriented: emphasizes institution-building, resilience, and effective responses to cyber threats, positioning capacity-building within governance and regulatory frameworks (European Commission, 2018; Barbero & Berglund, 2021).

The main problem with these traditional conceptual frameworks is that they consider only interstate capacity building activities from a donor towards a recipient (beneficiary) country. However, it can occur between different types of actors and recipients, including non-state actors as well. They also obscure the multidirectional flows of resources, expertise, political capital, and legitimacy that characterize many cyber capacity-building partnerships.

Cyber capacity-building has become a key interface between Global North and Global South actors, where digital inequalities, development priorities, and geopolitical interests intersect. Most large-scale initiatives are still funded and coordinated by actors in the Global North, while a significant share of recipient countries is located in the Global South. Cyber capacity-building can enhance institutional development, workforce training, and cyber resilience in Global South contexts; yet it may also perpetuate hierarchical relationships, influence domestic policy agendas, and establish new kinds of digital reliance (Chang& Coppel, 2020). Cybersecurity frameworks provided by external entities may synchronize the legal systems,

infrastructures, and institutional priorities of recipient states with the preferences of donors, thus connecting capacity-building to wider dynamics of influence, conditionality, and norm diffusion within the global digital landscape. Cybersecurity frameworks introduced through external assistance can align the legal systems, infrastructure and institutional priorities of beneficiary states with the preferences of donors. This links capacity building to the broader dynamics of influence, conditions and norms in the global digital order (Carver, 2025).

Cybersecurity capacity-building projects, however, are not only technical assistance projects anymore, as they have strengthened links to foreign policy, security cooperation, regulatory outreach, and international norm-making (Collett, 2021). They are used to support cybercrime cooperation, incident response capabilities, policy coordination mechanisms, workforce development, and the establishment of national and regional cybersecurity institutions. Cyber capacity-building has been integrated within the framework of cyber diplomacy.

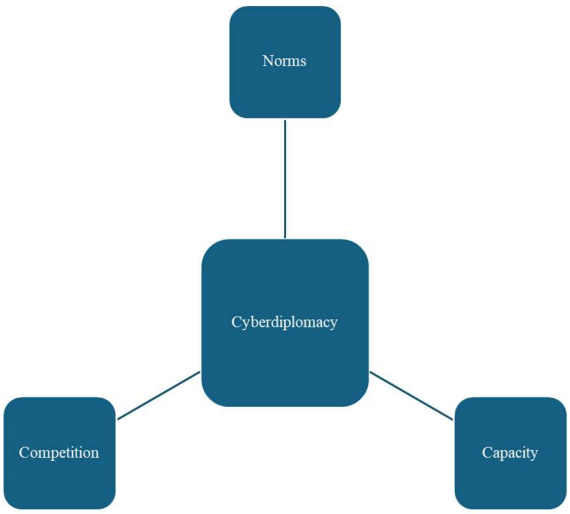
Historically, the distinction arose because "digital capacity building" was linked to traditional development goals and often avoided security language, while "cyber capacity building" was mostly limited to technical cybersecurity issues and treated as separate from digital development (Pawlak & Barmpaliou, 2023). Parallel to this division, there are two main explanations for why donors provide capacity building support. One is that support serves development and normative goals: development progress, humanitarian values, and the UN's sustainable development goals. At the same time, this logic is complemented by the fact that donors can promote preferred cyber norms through programs and secure institutional access for themselves through bilateral channels and socialization. The other explanation comes from cybersecurity literature: according to this, "cyber capacity building" increases the resilience of recipient countries to cyber risks, reducing the negative spillover effects of "weak links" in the global network (Gjesvik, 2023).

However, the explanatory power of both explanations is limited. On the one hand, there is no universally accepted distinction between "digital" and "cyber" capacity building: the meaning of the terms is context- and time-dependent, and in practice they are becoming increasingly blurred (Pohle & Voelsen, 2022). Development-oriented explanations deal better with selectivity, but both approaches reveal little about how geopolitical competition and pressures surrounding digital sovereignty shape aid decisions. The concept of "weaponized interdependence" (Farrell & Newman, 2019) provides a useful lens to interpret cyber capacity-building as a form of network-based power. While originally developed to explain coercion through global economic networks, its core insight—that structurally central actors can leverage asymmetric interdependencies—can be extended to capacity-building relationships. In this context, capacity-building does not merely reduce vulnerabilities but can also embed recipient actors within donor-centered institutional, technical, and normative networks. This perspective allows us to interpret cyber

capacity-building as a mechanism through which donors shape network structures and, potentially, create forms of dependency or alignment. Rather than direct coercion, influence is exercised through standard-setting, institutional design, and sustained engagement. This logic underpins the concept of competitive strategic alignment, whereby donors use capacity-building to position themselves within global cyber governance networks and align partner countries with their preferred norms and frameworks.

This framework also fits well with a broader interpretation of cyber diplomacy: cyber diplomacy is the diplomatic handling of cyber-related issues (negotiation, norm-setting, cooperation) with the aim of maintaining stability and promoting responsible behavior; it also supports capacity building in developing countries through knowledge sharing, training, and technology transfer, while keeping the balance between governance, rights, and security on the agenda (Radanliev, 2025).

Figure 1: Conceptual framework of cyberdiplomacy



Source: compiled by the author based on the literature (Radanliev, 2025).

Based on the literature cyberdiplomacy consists of the above three competing elements – namely norms including rules, standards, and their legitimacy; competition with great power dynamics centered around power and influence; and capacity including skills, infrastructure and institutions. Related to the norms, what we can see at an international level is that the United Nations OEWG dominated in norm setting, having a relatively rich network of collaborations (Shakeel et al., 2025). Regarding the cyberpolicy governance frameworks, there are two main approaches – one is state-centered followed by Russia and China, the other is a more network

centric approach followed by the European Union and the United States. Due to this shared approach towards cyber policy, a certain norm coalition can be studied between the European Union and the United States (Anagnostakis, 2021). Radanliev (2025) also points out that the lack of guiding norms in developing states can be a source of escalation of the instability, therefore the strategic interests of developed countries are also to offer a norm framework for developing countries. This can lead to an even more intensive competition along with the competing norm frameworks. Capacity building, however, is an efficient tool for strategic alignment (Carver, 2025), and can be a pure governance question (Muller, 2015). As a network aspect what can be studied is that after all, central actors with more developed frameworks and capacities form their own competing collaboration networks to share same norms, while the developing countries form digital peripheries and are in a submissive position (Carver, 2025). This great power competition is reflected in the United States approach, acknowledging that capacity building activities are not always the most attractive tools, but they play a key importance in how policy translates into real world outcomes such as increasing the state's competitiveness against rivalry challenges (Ford, 2020). Studying cyberdiplomacy, the study of strategies is crucial as they are the manifestations of the states' political will and attitudes (Urbanovics, 2022; Thomázy, 2021).

Methodology

The research used a mixed-methods strategy, including descriptive statistics and network analysis. The research is based on the data of the Cybil Portal, an international database of cyber capacity-building projects. Cybil was initiated by the Global Forum on Cyber Expertise (GFCE) to improve coordination, transparency, and efficacy in global cyber capacity-building initiatives. During the data collection period in November 2025, the database had 1,026 entries, encompassing projects, resources, and events. The analysis predominantly utilizes the "Projects" dataset, which records specific cyber capacity-building initiatives. However, it is important to note that there is no single definition of what can be included in cyber capacity building projects, therefore the states and international organizations are free to upload a huge variety of their ongoing or finished projects.

The data was collected from the official platform of the Cybil Portal. Extracted variables included geographic focus, donor and implementing actors, and thematic areas. I used descriptive statistical methods to analyze the global and regional distribution of projects. Meanwhile, network analysis was employed to map donor-recipient relationships and implementation partnerships to capture relational dynamics. This process helped to identify key actors, collaborative patterns and regional clusters within the domain. The networks were visualized and analyzed using Gephi 0.10.1. Ego networks centered on donor actors were constructed in order

to compare the positions and network structures of three key actors: the European Union, the United Nations and the United States.

To ensure analytical clarity, key concepts were operationalized as follows. "Cooperation intensity" is measured through edge weights, defined as the number of jointly implemented projects between actors. "Network centrality" is operationalized using weighted degree centrality, capturing the extent to which an actor is connected to others while accounting for the strength of these ties. Edge weights are measured by the number of joint projects, and were incorporated both into the layout algorithm and the calculation of network metrics. Weighted degree centrality was computed for all nodes and normalized by the maximum observed value to allow for clearer interpretation and comparison. The selection of weighted degree centrality is justified by the study's focus on collaboration intensity rather than brokerage or positional control. While alternative metrics such as betweenness centrality could capture intermediary roles, the present analysis prioritizes the identification of highly connected actors and dense cooperation patterns across networks.

Regarding the visualization of the networks, node size reflects the normalized weighted degree, indicating the relative connectedness of actors, while edge thickness relates to the strength of ties. Spatialization was produced using the ForceAtlas2 algorithm, with edge weights shaping attraction forces so that more intensive cooperation pulls nodes closer together. In addition to visual network interpretation, quantitative network indicators were used to support the analysis. Network density provides an indication of overall connectivity, while modularity helps identify the presence of subgroups or regional clustering.

Taken together, these methods make it possible to analyze cyber capacity-building not only as a set of technical interventions, but also as a structured field of geopolitical and diplomatic practice (Homburger, 2019). However, some limitations may arise as the Cybil Portal is based on voluntary reporting on data which introduces potential reporting bias. Furthermore, variation in how actors define and report "cyber capacity-building projects" may affect comparability across cases.

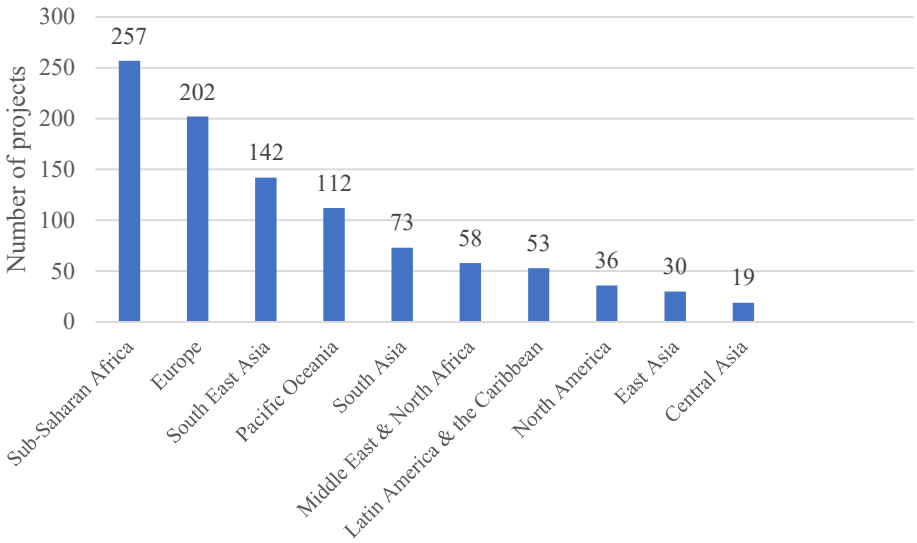
Cyber capacity building projects

This section presents the key findings on the patterns of cyber capacity building projects included in the Cybil Portal. First, general trends are presented, followed by a separate section highlighting the key characteristics of cyber capacity building projects coordinated by the EU, the United Nations and the United States.

General trends in cyber capacity building

First, the worldwide trends of cyber capacity building are presented.

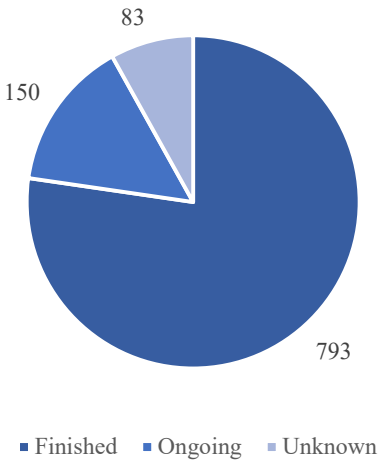
Figure 2: Regional breakdown by the number of cyber capacity building projects



Source: compiled by the author based on the data of the Cybil Portal.

Based on the number of CCB projects, we can study a regional breakdown led by a focus on Sub-Saharan Africa (257 projects), followed by Europe (202 projects) and Southeast Asia (142 projects). Altogether, the Cybil Portal dataset contains 1,026 projects, meaning that 25% focus on Sub-Saharan Africa and almost 20% deal with the European region. The fewest projects focus on Central Asia (19) and East Asia (30), which are separated from the Southeast Asian region in the dataset.

Figure 3: Number of projects by status



Source: compiled by the author based on the data of the Cybil Portal.

Of the CCB projects included in the dataset, 77% (793) have already been completed, 14.6% (150) are ongoing, and the status of 1% is unknown. However, studies show that the role of cyber capacity building has grown since the 2010s (Cyber Digital Europe, 2021). Nevertheless, studies indicate an increasing significance of cyber capacity building since the 2010s (Cyber Digital Europe, 2021).

Table 1: Main categories by the number of CCB projects

Main Category	Total	Subcategories (with number of projects)
Emerging Technologies	5	
Cyber Security Policy and Strategy	434	Strategies (164)
		National Assessments (170)
		CBMs, Norms and Cyberdiplomacy (105)
Cyber Incident Management & Critical Information Protection	437	National Computer Security Incident Response (304)
		Critical Information Infrastructure Protection (119)
Cybercrime	227	Cybercrime Training and Prevention (70)
		Legal Frameworks / Cybercrime Law (66)
Cyber Security Culture & Skills	244	Cyber Security Awareness (131)
		Education, Training & Workforce Development (140)
Cyber Security Standards	82	

Source: compiled by the author based on the data of the Cybil Portal.

Table 1 shows the main categories of CCB projects, organized by topic and main goal. Globally, most projects focus on either cyber incident management and critical information protection (437), or the development of cybersecurity policies and strategies (434). These two categories are followed by enhancing cyber security culture and skills (244) and preparing recipient countries against cybercrime (227). Digging deeper into these main categories reveals the composition of the subcategories that define the projects' specific objectives and operational tasks. Within the dominant category of cyber incident management and critical information protection, we find the establishment of computer national security incident response teams (304) and the development of critical information protection services (119). Within the development of cyber security policies and strategies, the subcategories are strategies, national assessment frameworks, CBM norms, and cyber diplomacy.

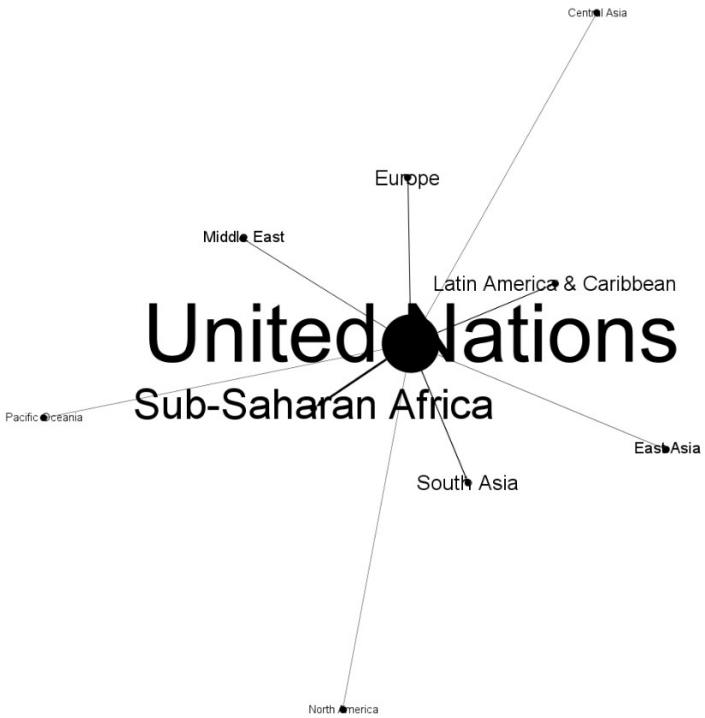
Global North actors-led cyber capacity building projects

Having carefully studied the general worldwide pattern of cyber capacity building, this section presents the actor-specific data. The three main actors involved in this comparison play crucial roles in cyber diplomacy. These are the United Nations, which introduced the report of the UN Group of Governmental Experts (GGE) in 2010, the United States, which is a cyber great power, and the European Union, which plays an active role in cyber diplomacy. Projects coordinated by these actors are primarily presented from a network-based perspective to highlight their main partners and recipients, and the status and main categories of these projects are also introduced.

Main regional focus points

Network analysis of cyber capacity-building initiatives linked to the United Nations (UN), the United States (US) and the European Union (EU) reveals that cyber capacity-building has become a key aspect of modern cyber diplomacy. Rather than being politically neutral forms of technical assistance, these initiatives are embedded in specific power, influence and governance constellations, reflecting broader foreign policy objectives and geopolitical logics.

Figure 4: Regional focus among United Nations-led CCB projects



Source: compiled by the author based on the data of the Cybil Portal.

Figure 4 shows the regional focal points of UN-led CCB projects. Based on this, the dominance of the Sub-Saharan African region can be seen, with 22 projects, followed by South Asia with eight projects and the Latin America and Caribbean region with seven projects. Of the 52 UN projects, 35 have been completed and 11 are ongoing. In terms of the main goals and instruments, there is a diverse picture, with an emphasis on developing cyber security strategies, primarily CBM norms and cyber diplomacy, as well as preparing recipients against cybercrime.

Studying the collaboration network graph, we can observe a very comprehensive and geographically inclusive structure covering all major regions of the world. This pattern aligns with conceptualizations of cyber diplomacy that emphasize multilateralism, norm entrepreneurship and capacity dissemination. The UN's broad geographical reach places it as a key factor in the cyber domain, promoting the dissemination of standards and best practices. This demonstrates the organization's institutional and normative power, as it influences the cybersecurity agenda by incorporating specific interpretations of cyber risk, responsibility, and governance into capacity-building initiatives, rather than using hard power.

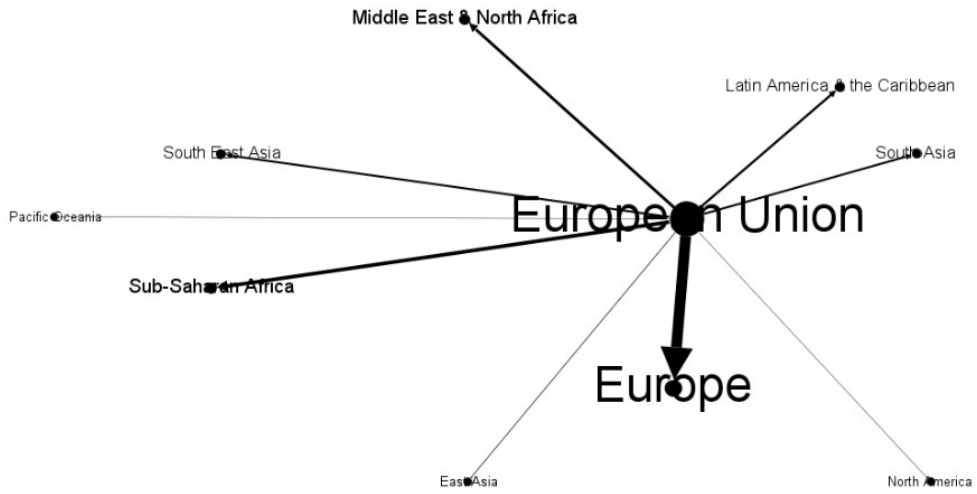
Figure 5: Regional focus among United States-led CCB projects

Source: compiled by the author based on the data of the Cybil Portal.

Figure 5 demonstrates the breakdown of United States-coordinated CCB projects. The regional breakdown shows a dominant focus on Europe (27 projects), followed by South Asia (26 projects) and Sub-Saharan Africa (14 projects). Of the 74 projects, 45 have been completed and 25 are ongoing. The main goals of the projects are cyber incident management and critical information protection (40%), and cyber security culture and skills development (36%).

Studying collaboration patterns, the great power logic is present in the US CCB activities and the selection of regions. The US is active in this field primarily in strategic regions such as Sub-Saharan Africa, Europe, East Asia and the Middle East. This concentration of specific regions and a less active global engagement in others reflects a cyber diplomacy approach wherein capacity creation facilitates alliance preservation, strategic rivalry, and security collaboration. This resembles international literature as CCB projects are often used to stabilize strategic partner regions. This functions as a relational power including the enhancement of dependency networks, development of interoperability, and the integration of recipient governments into US-favored cybersecurity frameworks. The significance of geopolitically important regions suggests that US cyber capacity development is linked to overarching national security and foreign policy goals, reinforcing the notion that cyber diplomacy serves as a tool for exerting influence in both digital and geopolitical spheres.

Figure 6: Regional focus among European Union-led CCB projects



Source: compiled by the author based on the data of the Cybil Portal.

Figure 6 summarizes the regional focus of the CCB projects coordinated by the European Union. There is a clear emphasis on the European region (including the Eastern Partnership countries), with 45 projects. This is followed by Sub-Saharan

Africa (16 projects) and the Middle East (13 projects). 66 projects have been completed and five are ongoing. These projects mainly focus on cyber security policies and strategies (44), particularly the development of CBM norms and cyber diplomacy, followed by cyber incident management and critical information protection. Data reveals that the establishment of National Computer Security Incident Response Teams is the most prominent subcategory with 25 projects.

The EU network is characterized by a strong regional focus, with Europe as the dominant hub and significant connections to Sub-Saharan Africa and the Middle East and North Africa. This regional concentration reflects the EU's characteristic mode of cyber diplomacy, which is based on regulatory, institutional and infrastructural forms of power. Within the EU and its neighborhood, cyber capacity-building serves several reasons: 1) consolidates governance frameworks, 2) harmonizes regulatory practices and 3) extends EU cybersecurity norms beyond its borders. In this sense, EU cyber capacity-building demonstrates how cyber diplomacy can operate as a governance technology, exerting influence through standard-setting, institutional design and long-term capacity integration rather than overt strategic alignment.

Table 2: Comparison of the characteristics of CCB projects led by the main actors involved in the analysis

Dimension	United Nations (UN)	United States (US)	European Union (EU)
Dominant cyber diplomacy logic	Multilateral, development-oriented cyber diplomacy	Strategic and security-oriented cyber diplomacy	Regulatory and governance-oriented cyber diplomacy
Geographic structure of network	Globally expansive and inclusive	Global reach with selective regional concentration	Regionally embedded and spatially concentrated
Primary regional focus	Sub-Saharan Africa; broad Global South coverage	Sub-Saharan Africa, Europe, East Asia, Middle East	Europe (dominant); Sub-Saharan Africa; Middle East
Form of power exercised	Normative and institutional power	Relational and strategic power	Regulatory and infrastructural power
Function of capacity-building	Diffusion of global norms, standards, and best practices	Strengthening alliances, interoperability, and strategic presence	Harmonization of frameworks, institutional integration, regulatory diffusion

Cyber assistance as power mechanism	Embeds UN norms and multilateral governance models	Constructs dependency networks and strategic alignments	Extends EU governance models and regulatory ecosystems
Relationship to geopolitics	Indirect; mediated through multilateralism and development discourse	Direct; closely aligned with national security and geopolitical competition	Structural; exercised through governance, neighborhood policy, and external action
Overall interpretation	Cyber capacity-building as normative cyber diplomacy	Cyber capacity-building as strategic cyber diplomacy	Cyber capacity-building as governance-driven cyber diplomacy

Source: compiled by the author.

Table 2 summarizes the main characteristics of these CCB projects led by the three actors involved in the analysis. First, we found diverse diplomatic logic exercised by each actor. The United Nations has a central focus on multilateral cooperation and aims to provide a forum for the development of cyber diplomacy. Meanwhile, the United States has a strategic and more security-oriented approach to cyber diplomacy, and the European Union uses the CCB projects for its regulatory and norm promotion efforts. The geographic scope of the actors differs as well. While the United Nations has a globally inclusive and wide collaboration network and a broad Global South coverage, the other two actors rather focus on their partner regions which are under their influence. For the United States, Sub-Saharan Africa, Europe, East Asia and the Middle East are all important partners as a great cyber power. Opposite to this, the European Union primarily focuses on European countries, and their very limited spheres of influence including Sub-Saharan Africa and the Middle East.

The rationale differs, too. While the United Nations uses CCB projects to diffuse global norms and develop best practices, the United States considers them instruments for strengthening alliances and enhancing its strategic presence. The European Union's approach is similar to that of the United Nations, as its primary goal is to harmonize frameworks and promote institutional integration. UN-led CCB projects have strong normative and institutional power, US projects have strategic significance for the country and EU-led projects have infrastructural power. UN-led cyber capacity building is indirectly associated with geopolitics, functioning mostly through multilateralism, development frameworks, and norm diffusion, which aligns with a type of normative cyber diplomacy. US Cyber capacity-building is directly embedded in national security and geopolitical competition, framing capacity-building as an instrument of strategic cyber diplomacy. The EU takes a structurally embedded approach, exercising cyber capacity-building through

governance, regulatory power, and neighborhood policy, reflecting a model of governance-driven cyber diplomacy.

Conclusion

This article examined cyber capacity building as a practice of cyber diplomacy through a network analysis of projects coordinated by the United Nations, the United States, and the European Union. The results show that cyber capacity building is not a politically neutral form of technical assistance, but a structured, geopolitical, normative, and governance-oriented practice in which power can be exercised through institutional, relational, and infrastructural means.

Although all three actors use cyber capacity building as a foreign policy tool, they do so in significantly different ways. Results pointed out that UN-led initiatives function primarily on a multilateral basis and emphasize the dissemination of norms, which aligns with the normative cyber diplomacy model. US-led projects are closely embedded in strategic competition and alliance politics, reflecting a form of strategic cyber diplomacy. In contrast, EU-led initiatives focus on regulatory coordination, institutional integration, and neighborhood governance, which reflects governance-oriented cyber diplomacy. These findings carry significant implications for the comprehension and assessment of cyber capacity-building in international policy discussions. They propose that such projects be evaluated not only for their performance but also concerning the political and governance frameworks they incorporate.

Regarding the EU network, Europe can be seen as the primary hub, complemented by involvement in Sub-Saharan Africa and the Middle East and North Africa. This design embodies the EU's overarching external action framework, wherein internal integration, neighborhood stabilization, and development cooperation are included. In the cyber domain, capacity-building expands this concept into the digital realm, framing cybersecurity as an issue of governance rather than only of security. From the perspective of EU cyber diplomacy, these results support interpretations of the EU as a regulatory and normative power. Cyber capacity-building facilitates the dissemination of EU-endorsed standards, institutional frameworks, and policy structures, integrating cybersecurity into broader initiatives of digital transformation, rule of law, and institutional change. Results show that the EU cyber diplomacy focuses on the establishment of a regional cyber framework, where partner countries involved in CCB projects are harmonized from a governance and regulatory aspect, and external engagement through CCB also aims to reinforce the same governance model. This discovery aligns with research on EU external governance and regulatory authority, emphasizing the Union's ability to influence policy contexts via technical support, institutional collaborations, and conditional cooperation.

The significance of cyber capacity-building in Global South contexts prompts essential inquiries. Although these initiatives may facilitate institutional development, skills acquisition, and cyber resilience in the partner countries targeted by these projects, they raise questions related to power and influence of the donor country. Namely, to what extent do these projects press the recipient countries towards adopting the donor countries' norms, danger perceptions and governance framework. The integration of cybersecurity into donor-driven frameworks poses a risk of generating new kinds of digital reliance, as recipient nations conform their legal systems, infrastructures, and policy priorities to external agendas.

The comparative analysis highlighted that cyber capacity-building is a very essential tool to develop and follow one's cyberdiplomacy governance model. For the EU, it facilitates the externalization of regulatory and governance frameworks; for the United States, it strengthens strategic alignment and security alliances; and for the United Nations, it institutionalizes global standards and inclusive structures. In all three instances, cyber aid functions as a means of structuring cyberspace via networks of financing, standards, and institutional collaborations.

References

Anagnostakis, D. (2021). The European Union–United States cybersecurity relationship: A transatlantic functional cooperation. *Journal of Cyber Policy*, *6*(2), 243–261. https://doi.org/10.1080/23738871.2021.1916975

Barbero, F., & Berglund, N. (2021). Cybersecurity capacity building and donor coordination in the Western Balkans. DCAF. https://www.dcaf.ch/sites/default/files/imce/Events/CybersecurityConference_DiscussionPaperPanel%203_CapacityBuildingDonorCoordination.pdf

Carver, J. (2025). Developing digital "peripheries" for strategic advantage: Capacity building assistance and strategic competition in Africa. *Contemporary Security Policy*, *46*(3), 455–496. https://doi.org/10.1080/13523260.2024.2430021

Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 101959. https://doi.org/10.1016/j.cose.2020.101959

Collett, R. (2021). *Cyber capacity building: Trends and scenarios. EU Cyber Direct*. https://directionsblog.eu/cyber-capacity-building-trends-and-scenarios/

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy*, *6*(3), 298–317. https://doi.org/10.1080/23738871.2021.1948582

Connelly, S. (2007). Mapping sustainable development as a contested concept. *Local Environment*, *12*(3), 259–278. https://doi.org/10.1080/13549830601183289

European Commission, & High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace* (JOIN(2013) 1 final). Publications Office of the European Union.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Ford, C. A. (2020, November 20). The evolution of international security capacity building [Remarks]. U.S. Department of State. https://2017-2021.state.gov/the-evolution-of-international-security-capacity-building/

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. *Review of International Political Economy, 30*(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Hathaway, M., & Spidalieri, F. (2021). *Integrating cyber capacity into the digital development agenda*. Global Forum on Cyber Expertise Foundation.

Homburger, Z. (2019). The necessity and pitfall of cybersecurity capacity building for norm development in cyberspace. *Global Society, 33*(2), 224–242. https://doi.org/10.1080/13600826.2019.1569502

Hurel, L. M. (2021, April). *Cybersecurity in Brazil: An analysis of the national strategy* (Strategic Paper 54). Igarapé Institute.

Muller, L. P. (2015). Cybersecurity capacity building in developing countries: Challenges and opportunities (NUPI Report No. 3). *Norwegian Institute of International Affairs*. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/284124/NUPI+Report+03-15-Muller.pdf?sequence=3

Pawlak, P. (2014). Riding the digital wave: The impact of cyber capacity building on human development (*EUISS Report No. 21*). European Union Institute for Security Studies. https://www.iss.europa.eu/content/riding-digital-wave-%E2%80%93-impact-cyber-capacitybuilding-human-development

Pawlak, P. (2018). *Operational guidance for the EU's international cooperation on cyber capacity building*. European Union Institute for Security Studies.

Pawlak, P., & Barmpaliou, P.-N. (2023). *Operational guidance for the EU's international cooperation on cyber capacity building* (2nd ed.). European Union.

Pohle, J., & Voelsen, D. (2022). Centrality and power: The struggle over the technopolitical configuration of the internet and the global digital order. *Policy & Internet, 14*(1), 13–27. https://doi.org/10.1002/poi3.296

Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. *Journal of Cyber Security Technology, 9*(1), 28–78. https://doi.org/10.1080/23742917.2024.2312671

Seidl, T. (2024). Charting the contours of the geo-tech world. *Geopolitics, 29*(5), 1–13. https://doi.org/10.1080/14650045.2024.2333358

Shakeel, M. B., Urooj, B., Imran, M. S., & Abbas, M. J. (2025). Toward a new cyber world order: Cyber diplomacy and the changing nature of international relations. *Policy Research Journal, 3*(10), 658–668.

Thomázy, G. (2021). Migrációs stratégiák: Dél-Amerika vs. Európa: Ecuador, Kolumbia, Magyarország és Spanyolország összehasonlító elemzése. *Hadtudomány, 31*(2), 58–74. https://doi.org/10.17047/HADTUD.2021.31.2.58

United Nations. (2002, May 14). United Nations system support for capacity-building (E/2002/58). https://www.un.org/esa/documents/ecosoc/docs/2002/e2002-58.pdf

Urbanovics, A. (2022). Cybersecurity policy-related developments in Latin America. *AARMS – Academic and Applied Research in Military and Public Management Science, 21*(1), 79–94. https://doi.org/10.32565/aarms.2022.1.6

Urbanovics, A. (2023). Cybersecurity strategies in the Visegrád countries: A cross-country analysis. *Nemzet és Biztonság: Biztonságpolitikai Szemle, 16*(2), 100–113. https://doi.org/10.32576/nb.2023.2.7

Wilén, N. (2009). Capacity-building or capacity-taking? Legitimizing concepts in peace and development operations. *International Peacekeeping, 16*(3), 337–351. https://doi.org/10.1080/13533310903036392