Peer Review Session 1

Andrew Galea Roberts

Part I. Reflection

My topic: EU & Cyber Diplomacy

So far, the first stage of my research is going quite well. I have started mostly with reading sources about the topic as well as about my framework. As the topic is not very old (mostly developed in the last 20 years) there are not too many sources, which on the one hand makes it not too overwhelming to research, but on the other hand it could make it difficult to fit into the framework I would like to use. I have also managed to find a niche within the topic that will help me address the gap part of my thesis, as a fair few papers already focus on the sanctions part of my topic. I also think my research is going quite well because I enjoy the readings and the topic itself.

I am concerned, however, on how I am going to justify how I have narrowed down my topic, that is, only taking a subset of the aspects of diplomacy in this context, as I think I may not have enough space to also deal with the sanctions aspect of EU cyber diplomacy. This is also the most publicly visible and publicised aspect, but I am not sure it is too useful for tracking the EU's effectiveness. There is also the question of whether there is enough data and evidence for my findings to have any meaning, or whether I will have to take a different approach if there simply is not enough EU action in the area.

As so far I have only had an introductory meeting with my supervisor, I have not had too much in terms of feedback, but I have been guided on some questions I could ask to find a research question.

Part II. Input

Topic Area

The topic I am researching is the EU's cyber diplomacy efforts, specifically those that are more preventative in nature (such as capacity-building, cyber dialogues (Pawlak, 2025)). I may focus on bilateral efforts and the EU's Cyber Diplomacy toolbox, which is a framework for diplomatic responses to Cyber incidents that was agreed in 2017 and amended in 2023, or I might focus on the EU's role in UN negotiations of cyber norms.

I think it is interesting and relevant because cybersecurity is increasingly having an effect on both our lives as well as states' relations between one another (Dunn Cavelty, 2025). Ever since the beginning of the internet era, the EU has acted to promote its values through the governance of the internet in general, and this has been extended to cybersecurity more recently. The EU has adopted legislation to improve cybersecurity, in critical sectors for example through the 2016 NIS Directive (Kasper et al., 2021), but coordinated action between Member States towards Third States (or International Organisations) is naturally more difficult, in part because of the intergovernmental nature of EU Foreign Policy.

Research Gap and Research Questions

The main gap that I have identified is tracking the effectiveness of specific Cyber diplomacy efforts by the EU. Certain authors have clearly outlined the tools available to the EU (for example Bendiek, 2018 or Pawlak, 2025), including specific cases. Another has outlined the role the EU has played over time on a global stage (Calderaro, 2024), but none of these have traced specific outcomes to EU action similarly to Schunz (2021). In this chapter, Schunz describes a framework for analysing the effectiveness of EU External Action, and then applies it to the sphere of climate action. This framework consists of four steps: identifying EU objectives; matching objectives with outcomes; tracing EU external action; and determining the degree of EU external effectiveness. My research would aim to do similarly, but for cybersecurity. In terms of Smith's (2016) work on categorising the approaches to the analysis of EU Diplomacy, I would thus work through a 'power, persuasion and norms' approach. I think this could be useful because it would aim to track whether the EU has an effect on these relationships in a practical way, beyond the normative aspirations that the EU has in general. I am still unsure whether to focus on bilateral efforts or multilateral efforts, as Schunz does in his work.

In the latter case, I could use the negotiations of the UN Convention against Cybercrime (United Nations Office on Drugs and Crime, n.d.) or EU coordinated effort in the UN Group of Governmental Experts on Cybersecurity meetings , which is a smaller group, but which always has an EU member state present due to France's Security Council status (Council on Foreign Relations, 2015). In this case, my research question could be *'Is the EU effective in influencing Cybersecurity norms at a multilateral level?'*.

On the other hand, I could also focus on the cooperation between the EU and a third state, such as through analysis of cyber dialogues, capacity building and assistance (European External Action Service, 2026). A larger scale example of this is 'Cybersecurity Policy in the EU and South Korea from Consultation to Action' (Boulet et al., 2022), which is a book about the cybersecurity interactions between the EU and South Korea. I would probably focus on a neighbourhood third-state, such as Ukraine or Moldova, where EU action is relatively broad in general, but also in the cyber domain (Pawlak, 2025, outlines the measures taken with these countries). My research question could thus be *'How effective is the EU's cyber diplomacy towards Ukraine?'*. I am concerned that finding data and evidence for the effects of bilateral diplomacy may be more difficult than in a multilateral setting, as the outcomes in bilateral diplomacy may not be as clear as a resolution or a conclusion from a multilateral forum for example.

Use of GenAI

I tried using Research Rabbit with some of my sources and it was not able to process them. As a result, so far I have not used any GenAI tools. Most of my sources have been found through Google Scholar.

References

Bendiek, A. (2018). The European Union's foreign policy toolbox in international cyber diplomacy. *Cyber, Intelligence, and Security*, *2*(3), 57–71.

Boulet, G., Reiterer, M., & Pacheco Pardo, R. (Eds.). (2022). *Cybersecurity policy in the EU and South Korea from consultation to action: Theoretical and comparative perspectives*. Palgrave Macmillan Cham. https://doi.org/10.1007/978-3-031-08384-6

Calderaro, A. (2025). The EU as a global cyber actor. In S. Lucarelli & J. Sperling (Eds.), *Handbook of European Union governance* (pp. 540–553). Edward Elgar Publishing. https://doi.org/10.4337/9781803925189.00053

Council on Foreign Relations. (2015, April 15). *The UN GGE on cybersecurity: What is the UN's role?* https://www.cfr.org/articles/un-gge-cybersecurity-what-uns-role

Dunn Cavelty, M. (2025). *The politics of cyber-security.* Routledge. https://doi.org/10.4324/9781003497080

European External Action Service. (2026, July 10). *Cybersecurity*. https://www.eeas.europa.eu/eeas/cybersecurity_en#129026

Kasper, A., Osula, A.-M., & Molnár, A. (2021). EU cybersecurity and cyber diplomacy [Ciberseguridad y ciberdiplomacia de la UE]. *IDP: Revista de Internet, Derecho y Política*, 34, 1–15. https://doi.org/10.7238/idp.v0i34.387469

Pawlak, P. (2025). The European Union as a cyber diplomacy actor. In G. Christou, L. Käser, & S. Rheinbay (Eds.), *The Palgrave handbook on cyber diplomacy* (pp. 781–802). Springer Nature. https://doi.org/10.1007/978-3-031-93385-1_36

Schunz, S. (2021). Analyzing the effectiveness of European Union external action. In S. Gstöhl & S. Schunz (Eds.), *The external action of the European Union: Concepts, approaches, theories* (pp. 182–199). Bloomsbury Publishing.

Smith, M. (2016). European Union diplomacy. In C. M. Constantinou, P. Kerr, P. Sharp & M. Smith (Eds.), *The Sage handbook of diplomacy* (pp. 308–317). Sage. https://doi.org/10.4135/9781473957930.n26

United Nations Office on Drugs and Crime. (n.d.). *United Nations Convention against Cybercrime*. United Nations. Retrieved October 22, 2026, from https://www.unodc.org/unodc/en/cybercrime/convention/home.html

Peer Review Session 2

Andrew Galea Roberts

Part I. Reflection

I think my research is going rather well, in that I have found a source of information, and a niche that I can write about that I think will be relevant and useful. As I will elaborate in the research gap section, I will likely focus on the outcomes of the *UN Open-ended Working Group on security of and in the use of information and communications technologies*, which met over eleven sessions between 2021 and 2025, and specifically on the EU's effectiveness during this process. Of course, I am still awaiting my supervisor's opinion and I have a lot of information to analyse, so I am looking forward to my next meeting to confirm that it will be a viable analysis. I have not advanced so much on the theoretical front, as I was focusing on finding the actual evidence to analyse.

I have taken some useful feedback from the first peer review session, notably that I should better highlight the importance and relevance of my topic. I thought this was especially useful as I might forget to include some of the basics while getting lost in the research. I was also advised to narrow down my topic, which I hope to have done this week.

Part II. Input

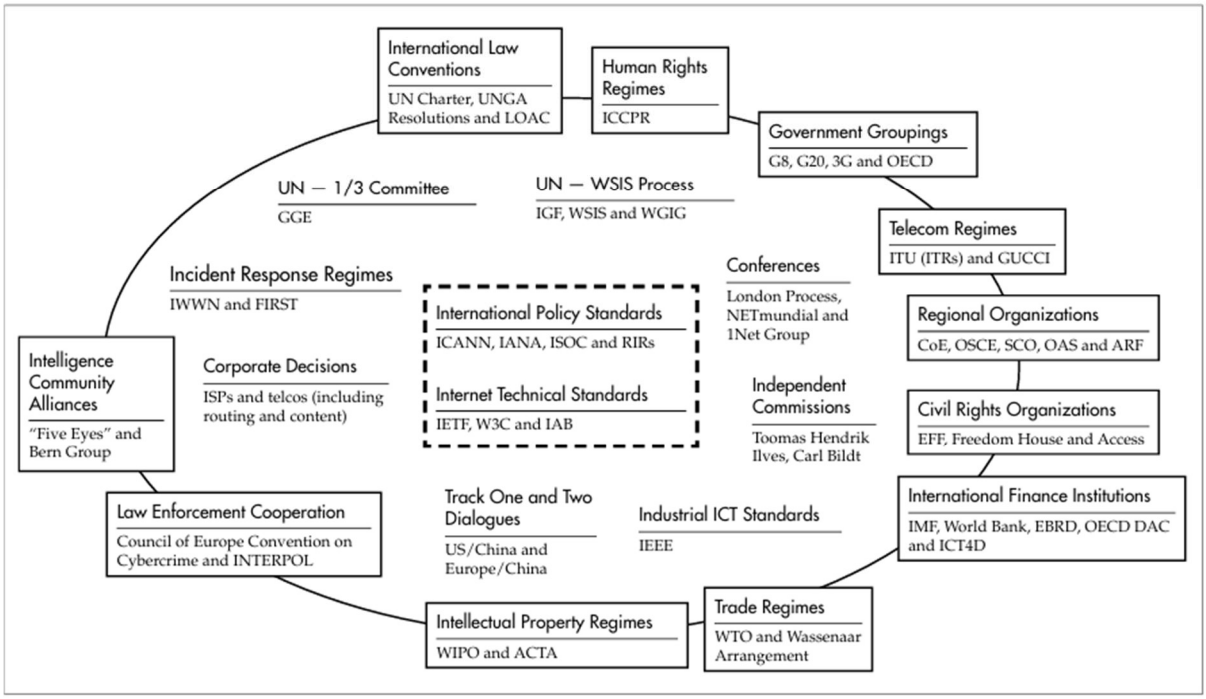
Research Gap and Research Question

I have for the most part focused on the same research gap as in the last Peer Review Session. I will focus on the EU's cyber diplomacy, and will aim to analyse the effectiveness of the EU as an actor on the global stage. The literature on EU cyber diplomacy does not examine specific outcomes of EU action but is largely descriptive, with respect to tools available to the EU (for example Bendiek, 2018 or Pawlak, 2025) or the evolution over time (Calderaro, 2024). My research will aim to explore what the EU has achieved (or not achieved) throughout an important UN process, to better understand and improve its foreign policy record (as in Schunz, 2021).

The process that I wish to trace, the *UN Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025*, is significant because it concluded with the creation of a permanent mechanism to house discussions on state behaviour in Cyber, within the UN. Previously, any negotiations were conducted either in an open ended working group (which was open to all UN Member States) or a group of governmental experts (GGE, which had a selective membership), both of which were only established by the General Assembly for a limited time period (Weber, 2025; Council on Foreign Relations, 2015). The main debates in these fora are on the applicability of international law in cyber, as well as the creation of a cyber treaty (Payne, 2025).

Since this process concluded recently, there is not much scholarship on the EU's role in this particular UN framework, but my research will build on existing literature on the EU's external action at the UN in general. The EU's record is 'mixed' at the UN (Keukeleire & Delreux, 2022), and my research aims to analyse how well the EU performs in the cyber domain.

Figure 1: The Regime Complex for Managing Global Cyber Activities



Source: Nye, 2014

The UN is not the only forum in the Cyber regime complex, however, it is important for two reasons. Firstly, my research will focus on states' (and the EU's) role in cyber more than corporate or standards aspects of Cybersecurity, and thus the UN is the natural venue. The UN GGE format had been recognised as the 'most reputable platform for agreeing international norms for States in cyberspace' (Ott & Osula, 2019; also reflected in diagram above), though it has not been renewed after 2021. The OEWG and now the permanent mechanism have taken its place.

Furthermore, the UN is 'considered as a central point of reference in the foreign policy of the EU' (Keukeleire & Delreux, 2022, p.334), and thus is a useful venue to investigate EU diplomacy.

Thus, my research question will be: *'How effective is the EU's cyber diplomacy at the multilateral (UN) level?'*

This research question will aim to fill the gap outlined above by analysing the outcomes of the most recent (and important) UN process in the cyber domain by applying Schunz' framework for 'assessing the effectiveness of the external action of the European Union'.

Theory

My theoretical framework is not as developed as other parts of my research, though I have some ideas on which theories to use.

The theory of EU actorness, whereby one must analyse the EU's 'capacity to behave actively and deliberately in relation to other actors in the international system' (Sjöstedt, 1977, as cited in Klose, 2018), offers a useful layer of analysis on top of the methodological approach, by framing the outcomes in terms of both the internal and external determinants that allow or do not allow the EU's objectives to be met (Petri et al., (2025). It could help to formulate a hypothesis on the overall effectiveness of the EU which is then confirmed or refuted by the research. An advantage

of this theory is that it will allow my research to unpack the EU's action, in that the methodology does not explore the factors contributing to the outcomes, only the causation, while these factors remain relevant to explaining the EU's effectiveness.

Methodology

My research will take a qualitative approach, based on a case study and using process-tracing, to evaluate the effectiveness of the EU's cyber diplomacy.

The analysis will be based on the framework developed by Schunz (2021), which includes four steps: identifying EU objectives; matching objectives with outcomes; tracing EU external action; and determining the degree of EU external effectiveness.

Process-tracing, as formulated by Beach and Pedersen (2019) allows one to identify the causal mechanisms between the EU's diplomatic initiatives and the decisions take at the OEWG. This method is particularly useful because it aims to isolate the effects of the EU from those of other international actors.

The research will be based particularly on document analysis of EU declarations and propositions, transcriptions of the OEWG sessions, and the final reports of this body. A chronological comparison of EU positions and results of negotiations can help identify convergences.

This approach has the advantage of going beyond a simple evaluation of the EU's normative ambitions, by empirically examining contributions made at a multilateral level, notably in the creation of the permanent mechanism.

Use of GenAI

So far I have not used GenAI tools for my research, except for researching theories for this paper, as most of my readings and sources do not include much in terms of theoretical basis so far, and writing this paper was time restricted. Additionally, a third party site with transcriptions of the OEWG Cyber sessions did use AI for some of the transcriptions. Whether I find a better alternative for my research is yet to be seen.

References

Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines* (2nd ed.). University of Michigan Press. https://doi.org/10.3998/mpub.10072208

Bendiek, A. (2018). The European Union's foreign policy toolbox in international cyber diplomacy. *Cyber, Intelligence, and Security*, *2*(3), 57–71.

Calderaro, A. (2025). The EU as a global cyber actor. In S. Lucarelli & J. Sperling (Eds.), *Handbook of European Union governance* (pp. 540–553). Edward Elgar Publishing. https://doi.org/10.4337/9781803925189.00053

Council on Foreign Relations. (2015, April 15). *The UN GGE on cybersecurity: What is the UN's role?* https://www.cfr.org/articles/un-gge-cybersecurity-what-uns-role

Keukeleire, S., & Delreux, T. (2022). *The foreign policy of the european union*. Bloomsbury Publishing Plc.

Klose, S. (2018). Theorizing the EU's Actorness: Towards an Interactionist Role Theory Framework. *Journal of Common Market Studies*, *56*(5), 1144–1160. https://doi.org/10.1111/jcms.12725

Nye, J. S., Jr. (2014). *The regime complex for managing global cyber activities* (Global Commission on Internet Governance Paper Series, No. 1). Centre for International Governance Innovation; Chatham House. https://www.cigionline.org/static/documents/gcig_paper_no1.pdf

Ott, N., & Osula, A.-M. (2019). *The rise of the regionals: How regional organisations contribute to international cyber stability negotiations at the United Nations level* (2019 11th International Conference on Cyber Conflict). NATO Cooperative Cyber Defence Centre of Excellence. https://doi.org/10.23919/CYCON.2019.8756863

Pawlak, P. (2025). The European Union as a cyber diplomacy actor. In G. Christou, L. Käser, & S. Rheinbay (Eds.), *The Palgrave handbook on cyber diplomacy* (pp. 781–802). Springer Nature. https://doi.org/10.1007/978-3-031-93385-1_36

Payne, R. (2025, July 24). *The OEWG ends and a new UN cybersecurity permanent mechanism is born*. Global Partners Digital. https://www.gp-digital.org/the-oewg-ends-and-a-new-un-cybersecurity-permanent-mechanism-is-born/

Petri, F., Blockmans, S., Drieskens, E., & Ergenc, C. (2025). *Actorness in different shades? Comparing EU external action across global governance institutions* (Report No. 27). Ensured. https://cdn.prod.website-files.com/65f94def12935f07cab6eb39/693a860281402ed00d559386_Report_9.1_public.pdf

Schunz, S. (2021). Analyzing the effectiveness of European Union external action. In S. Gstöhl & S. Schunz (Eds.), *The external action of the European Union: Concepts, approaches, theories* (pp. 182–199). Bloomsbury Publishing.

Weber, V. (2025). *A lack of action in UN cyber discussions is partly the fault of the West* (DGAP Memo, 36). German Council of Foreign Relations e.V. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-110658-9