SHIFTING FROM KINETIC TO CYBER: A CYBER DIPLOMACY LITERATURE REVIEW

Solana Beatriz AQUINO
University of the Philippines, Diliman Department of Political Science, Quezon City, Philippines
spaquino2@up.edu.ph

Abstract: The realm of cyber diplomacy is the new frontier of power relations and requires an evolution of our previous understanding of power dynamics in the international sphere. From the birth of cyber diplomacy in 2007, there have been attempts to create cyber diplomatic policies. However, the current literature has found unrealistic cybersecurity expectations for states and some with aggressive stances. We use a literature review to comb through various states' cyber stances, review their cyber readiness, and evaluate the neorealism principles underlying these moves. The United States and Russia are the current great cyber powers with North Korea, Singapore, Estonia, South Korea, Israel, and Iran catching up with their cyber policies. There is still a gap in the literature about the place of multinational companies that hold a large sway on cyberspace and more on the neorealist underpinnings of this new space.
Keywords: Cyber diplomacy, Cyberspace, Cybersecurity, Literature review, Neorealism.

INTRODUCTION

The transition from traditional diplomacy to cyber diplomacy in the second age of the Internet or the Fourth Industrial Era was inevitable. The realm of cyber diplomacy is the new frontier of power relations and requires an evolution of our previous understanding of power dynamics in the international sphere.

With the scale and speed of technological advancement, the shift from physical to cyberspace was inevitable. The level of interconnectivity and the change in the dynamic of human interaction, seamlessly offline and online, has paved the way for a new cyber frontier for nation-states to push their interests and conceptualize them in the contemporary world. By comparison to traditional physical domains, cyberspace is both complex and evolving. There is no definite domain space and it is more anarchical than traditional international relations. Thus, there is a gap to be filled by nation-states in defining their presence online. According to the Australian Institute of International Affairs, a broad definition of cyber diplomacy is the "use of diplomatic tools and initiatives to achieve a state's national interest in cyberspace that are commonly crystallized in the national cybersecurity strategies" (2021). However, cyber diplomacy also includes economic and human rights topics such as internet access, privacy, internet freedom, intellectual property, and the ethical use of digital technologies and trade (Goldman, 2021).

The birth of cyber diplomacy, according to Attatfa, Renaud, and De Paoli (2020), occurred in 2007 following a wide-ranging cyber-attack on Estonia. The attack crippled one of the most connected (in terms of wireless connectivity) countries by launching attacks that paralyzed several government and corporate sites. The escalation and severity prompted the discussion and realization that governments must start taking notice of their place in cyberspace and formulate policies to be enacted. It also highlighted that cyberspace has military and strategic

dimensions that are akin to traditional spaces that require diplomacy and coordination to keep balanced or to keep one's country safe, based on the principle of self-help. Cyber diplomacy will become a major component of foreign policy as global connectivity rises and its interdisciplinary nature evolves.

CYBERSECURITY AND DIPLOMACY IN NATO AND THE EU

Diplomacy faces a major challenge in this era as governments are constantly being pressured by multiple issues arising from the COVID-19 pandemic. Governments are realizing the importance of internet connectivity to power their economies, give them an edge in global competition, and promote internal stability, at the cost of exposure to cybersecurity issues. Other areas such as sustainable development, environmental concerns, and the global pandemic, the economy, and the evolution of international law also depend highly on both diplomacy and the ever-expanding use of cyberspace (Bodoni, 2020). The use of emerging technologies has also landed on the political agenda of several countries that may be termed cyberpowers, such the United States, China, Russia, France, Israel, and the United Kingdom, and active consumers (Attatfa, Renaud & De Paoli, 2020).

The Paris Call for Cyber Peace in 2018, a cyber initiative launched by France, highlights how the international community has taken notice of the importance of their place in cyberspace and the salience of cyber diplomacy. The Call was a key cyber diplomacy initiative that placed France at the forefront as international leader in cyber issues. There was a push for a soft power (power by cooptation) in the shaping of the initiatives in the Call. Three important points were highlighted in The Paris Call and in the French White Paper on Defence and National Security (2017): (1) Cybersecurity is a key issue in diplomatic relations; (2) A need to involve multiple public and private actors; (3) The need for international law to apply automatically in cyberspace.

Cybersecurity as a key issue was already internalized prior to the Call, by the cyber-attack on Estonia and the proliferation of other cybercrimes such as cyber-espionage, information leaks, and intellectual property theft. Security policymakers also recognized how devastating cyber-attacks can be, crippling information and communication networks, placing national economies and national security in jeopardy in mere seconds. In 2017, the EU adopted its Joint EU Diplomatic Response to Malicious Cyber Activities; however, it primarily stipulated that non-military instruments should be used. Bendiek (2018) points out that Europe would be "well-advised to adhere to the step-by-step cyber-diplomacy plan which is based on the principle of due diligence [...]" and pushes the need for better cyber-defence and retaliation capabilities. Currently, the EU's position is based on the resilience of its Members' digital infrastructures and cyber diplomacy so as to present itself as a force for peace. The increasing complexity and intensity of cyber-attacks that may or may not have a terrorism component cannot allow for a soft stance on cybercrime. They require a more proactive approach with advanced capabilities. The EU may continue with its stance as a force for peace in cyber diplomacy; however, there needs to be an upgrade in its cyber-defence strategy, at the very least.

The issue of using strong or offensive countermeasures is still up for debate as it is mired in political and legal issues. In 2016, Germany published its 2016 Cyber Security Strategy which included defensive cyber security and called for the creation of specialized task forces in the

Federal Office for Information Security, the federal police, and their intelligence agency. This goes against the 2017 EU 'force for peace' stance as it also includes a stance that requires military and strategic cyber weaponry and the creation of a legal basis for their use and deployment, citing the cyber-attacks on the federal parliament in 2015 and the government network in 2016. Bendiek (2018) counters the option of cyber-defence with cyber diplomacy. The definition of cyber diplomacy used in the study is as a tool for conflict de-escalation through international norm building, data protection, freedom of expression, and Internet Governance (Bendiek, 2018). With more than 30 states having commissioners for cyber foreign policy, the EU's new stance seems to be firm as a 'force for peace'. Critics note that many governments do not have the knowledge or the resources to uphold basic cybersecurity standards or detect if there are attacks using servers based on their territory. The capability-expectations gap may be too large at the current time. While critics do state that the EU has recognized the importance of a "free, open, and secure internet", they also advise that there needs to be more research into the cyber sanctions regime, based on the cyber diplomacy stance that they have adopted and is currently applied (Calleri, 2020).

NATO, by comparison, has classified cyber-attacks as a form of warfare which would fall under Article 5 of the North Atlantic Treaty's mutual defence clause. NATO also allows both defensive and offensive cyber-defence in the cases of self-defence or mutual defence (Bendiek, 2018). One of the earliest uses of its cyber-defence was in 2009 in retaliation to Iran where the US struck Iranian weapon assets with a cyberattack (Lancelot, 2020). In 2014, the Obama Administration imposed unilateral sanctions after a local Sony Corporation subsidiary fell victim to a cyber-attack that saw sensitive information copied. The US Administration's personnel data was illegally accessed during a large-scale cyber-attack just two years later. 2016 was also the year of the alleged presidential election interference by Russia. The US government sanctioned five companies and organizations as well as nineteen individuals for their participation. The security analysts in the US maintained their proactive stance well into 2021 and believe that strategic rivalry, proactive approaches, and embracing competition are still in their best interest (Goldman, 2021). However, critics argue that the development and deployment of these tools may foster mistrust, mutual insecurity, and conflict between nations (Bendiek, 2018).

CYBER DIPLOMACY AND THE MIDDLE POWERS

Japan and Australia in the Asia Pacific have also risen to these challenges, based on Manantan (2021) where he uses both countries as case studies. While both countries adhere to the cyber diplomatic tenets, in practice, there is an increase in the use of cyber deterrence measures. Japan, in particular, has aligned itself with the EU's stance through a number of bilateral agreements such as the EU-Japan Adequacy Decision on the Free Flow of Personal Information. The EUNITY Project also aimed to combine European and Japanese cybersecurity experts to analyze the policy framework about enhancing security, privacy, and innovation outside of the Union (Fantin, 2019). Australia, on the other hand, has released its 2020 Cyber Strategy with an increasing emphasis on the use of deterrent measures. Manantan (2021) argues that, as middle power states, their increasing reliance on deterrence instead of cyber diplomacy shows how they are bearing the brunt of the intensifying US-China power struggle. The dual approach to national cybersecurity is perhaps the most beneficial to both countries as it strikes a balance between cooperation and competition compared to the EU,

whose focus is on cooperation while the US pushes for competition. They are able to preserve the option for open dialogue and collaboration while maintaining their defences against the cyber-attacks or as, Manantan (2021) calls it, the cyber insecurity that the EU suffers from. Their agility and flexibility in their cyber policies put them ahead of other countries in this regard as we are all still coming to terms with the shaping and norming of behaviors in the cyber domain. Although the G20 has attempted to formulate acceptable behavior norms in cyberspace, actual practice is limited (Torres & Riordan, 2020). It is difficult to implement with states adopting a self-help posture in the wake of several devastating cyber-attacks and the continuous evolution of cyber tools and the emerging cyber powers.

The Kingdom of Saudi Arabia and Israel have also recognized the importance of cyber diplomacy and its role in cybersecurity. Saudi Arabia points to the lack and inefficiency of national policies and regulations surrounding cyber diplomacy to promote international cybersecurity. Alasmari (2021) argues that international cooperation is needed to create a multinational approach that establishes common policies and regulations, agreeing with Donaldson, Siegel, Williams, and Aslam (2015). Complex, enhanced diplomatic relations, particularly in the realm of cybersecurity must be pursued in order to safeguard against the increase in complexity and severity of cyber-attacks. While specific literature on Saudi Arabia's cyber practices is not as extensive as the EU or US literature, they seem to be leaning towards a deterrent-based model, similar to that of the US but with leniency, like Australia and Japan.

Israel is currently in its infancy with regards to cyber diplomacy as Pavel (2020) notes that policies and practice have not yet been fully adopted or implemented and practiced in Israel. However, unlike other nations, with the exception of Denmark, Israel has started to look for a 'cyber ambassador'. Evidence from their Ministry of Foreign Affairs sheds light on their adoption of new policies governing cyberspace. Israel, at the moment of writing, is leaning towards a more balanced view on deterrence and cooperation, similar to that of Australia and Japan.

RUSSIA'S EARLY LEAD IN CYBER POLICIES

Russia's cyber policies are more complicated to break down and are quite controversial. Russia has been the alleged perpetrator of multiple cyber-attacks and was even accused of interfering in the US presidential elections. In 2018, the European Union Institute for Security Studies (EUISS) published an issue on Russian Cyber Strategies. The issue compiles articles on Russia's cyber posture and case studies of particular cyber-attacks as well as EU and NATO reactions which were previously covered: they were not received well.

Russia has adapted a posture of offence being the best defence. Their history with cyber-attacks has been documented as early as 1986, when a hacker, "Hunter", attempted to break into the Anniston Army Depot in Alabama to extract information about the US Army Redstone Rocket test site. According to the research done by Popescu and Secrieru (2018), this is the first known cyber espionage operation engineered by the USSR in collaboration with East Germany against the US military. In 2000, Vladimir Putin signed the Information Security Doctrine, the first cyber policy document of its kind, detailing a list of broad threats including the major threat of "desire of some countries to dominate and encroach on the interests of

Russia in the global information space" (Soldatov & Borogan, 2018). The infamous Estonian attacks in 2007 were also perpetrated by the Russians, in particular Konstantin Goloskokov, who admitted in an interview that he was behind the attacks and pointing towards the Kremlin. Then, in 2013, Russia resurfaced in cyber affairs with its plan of creating "cyber troops". Russia's aggressive cyber-stance worked as a deterrent against neighboring countries and those whose actions ran against Russian interests. Russian cyber foreign policy turned responsive to crises and was applied tactically instead of strategically. This seemingly random application makes it difficult to anticipate and predict (Soldatov & Borogan, 2018).

Russia has also been accused of using trolls in their cyber-attacks. Kurowska and Reshetnikov (2018) sheds light on the Russian philosophy of the use of trolls. Instead of using classical propaganda, their strategy rests on creating cynicism to use as a weapon by disrupting normative foundations of key areas and principles of liberal governance. Kurowska and Reshetnikov (2018) point out that Pro-Kremlin trolls tend to be commissioned to perform specific tasks – thus, they are working to earn, not out of ideological reasons. The appropriation of trolling behavior to further government ideology is antithetical to original trolls whose goal is simply sowing disruption and frustration. The trolls create an environment that discourages political mobilization before it can materialize, through taunts and insults (Kurowska & Reshetnikov, 2018; Goolsby, 2019). Russia is well-equipped and tactical when deploying its aggressive cyber policies which makes it an effective deterrent and adversary in the cyber political sphere.

RECENT EVOLUTIONS IN THE CYBER ENVIRONMENT

The COVID-19 pandemic has shaken up our previous hierarchies of power and has increased the visibility of the 'self-help' principle in practice. Sarcinschi (2021) argues that our health resources, in particular vaccines, have been used as sources of hard power during one of the worst health crises we have faced in the last century. It is a redefinition of power based on resources used as diplomatic tools, in this case, the availability of protective aid and the distribution of vaccines. Sarcinschi (2021) also argues that the spectrum of power behaviors that states have exhibited to induce or coerce actors are typical of those found in traditional neorealist literature, despite the type of resource changing. However, Sarcinschi also acknowledges the boost of international cooperation through "vaccine diplomacy" or the distribution of vaccines as a diplomatic tool, there was also a rise in attempts to produce nationalistic sentiments which brought forth issues of competition for resources and vaccine nationalism. We have also witnessed classic neorealist behaviours from states such as the closure of international borders, international competition, the critique of the role and influence of the World Health Organization and deployment of military forces (Alhammadi, 2021). With the interests of their citizens in mind, states continue to prioritize an 'us first' mentality, based on the principle of self-help and a continued reluctance to international cooperation. The lack of coordination is proving to be a major barrier for collective international action and diminishes the influence of international organizations as states scramble to solve the economic repercussions brought about by the pandemic.

It is difficult to determine whether health resources will maintain their position as the new definition of power and whether power dynamics will truly shift or if it is a short-lived phenomenon that will disappear once the world settles down, if at all. However, vaccine

diplomacy highlights the evolution of our definition of power but still within somewhat traditional boundaries set by territory or intellectual claims.

There is also a shift from traditional conferences and forums to cyberspace to combat the rise of infection rates. This leads us to see a shift in power dynamics with the definitions of power rapidly changing in this new era. As more and more key areas of governance and economy go online in lockstep with the rapid development of technological infrastructure, it is inevitable that the new battleground for diplomatic action shifts online. Previous examples of Russia's cyber stance and the rest of the world starting to adopt principles of cyber diplomacy and cyber-defense show that the new face of power no longer rests on traditional military strength or possibly in the distribution of health resources but in the ability to secure national interests and in the security of government and economic infrastructure online. One very visible and current example is the rising Sino-American tension, pushed by both the COVID-19 pandemic and the alleged Chinese "provocations" in cybersecurity (Djedei & Kerboua, 2021). The American government, under President Joe Biden, has a more cautious approach towards China, starting with the decoupling of its economy, but China is not expected to back down and is predicted to be more aggressive in its economic interests, pushing for stronger and more varied types of cybersecurity, including with the purpose of deterrence. Goldman (2020; 2021) also argues that the United States will most likely continue its aggressive stance on cyber-defense, as previously seen in the NATO categorization of cyber-attacks as warfare activities. Both countries' competition for power no longer remains within the traditional boundaries of land, air, and sea, but extends towards cyberspace (becoming an official operational domain in 2016) and making their mark through their cybersecurity stances.

Minchev (2021) points out this pandemic has also highlighted the type of cyber behaviors that require stronger security and this shows the importance of cybersecurity strength as a means of power and control for states. Examples of recent cyber-attacks are related to the pandemic such as the water supply cyber-attack in Florida, which was unsuccessful, and pharmaceutical industry espionage related to vaccines (Minchev, 2021). These are complicating the security landscape and shifting our understanding of security from traditional patterns to cyberspace. Cybersecurity strategies have been implemented and adopted by several countries, although the gap between expectations and reality is quite large. The idea that resilience and cyber diplomacy may bridge this gap is a naive notion as the intensity and complexity of cyber-attacks increase and the motivation behind them changes and evolves from merely lone agents extorting ransom to trolling\disinformation\fake news to outright terroristic attacks (Lancelot, 2020).

THE CYBER ANARCHY

Our understanding of the international sphere is anarchic in a neorealist perspective but the cyber domain is even more anarchic, with the rules of sovereignty muddled. There are no territorial boundaries similar to the ones we have in the real world, unless we dead in the cyber-physical infrastructures underpinning cyberspace. Barrinha and Renard (2020) argue that cyberspace is post-liberal. Cyber power is used to create opportunities in other fields and to influence others. A state may use this aggressively or diplomatically. This gives rise to the opportunity to create new great cyber powers or those with "large or technologically advanced economies; public institutions that channel…the private sector; adventurous…

rapacious military and intelligence agencies...” (Barrinha & Renard, 2020). Although they hold that the US is a lone cyber superpower, we could point out Russia’s strong cyber power and capabilities as well as their tactical use, allowing Russia to stand beside the US, while China is catching up. Cyber power also allows countries with lesser power in other domains to step up in the world order such as Estonia, South Korea, and Singapore. Israel, Iran, and North Korea have been catching up on their integration of cyber tools in their military operations. However, this also begs the question of multinational companies that hold a large sway over the tools we use today, such as Google, Amazon, Facebook’s Metaverse, Apple, and Microsoft. Although they are technically not sovereign states, they hold massive power in cyberspace and beg the question as to their role in internet governance in this anarchic sphere.

CONCLUSION

Cyber diplomacy is a new field and a new frontier in international relations and studies. More studies and systematic literature reviews should be undertaken to see the true effects of cyber diplomacy on the power dynamics and the shifts that come with it. There is currently a gap in literature regarding the subject. Studies or reviews have not yet been undertaken about where power structures lie and where the new dynamics of cyberspace are leading. How will they affect our current understanding of international relations theories which are mainly based on traditional spaces? There are still several theoretical and practical questions to study in this new frontier.

The evolution of cyberspace, the increasing use and importance of cyber diplomacy, and the shifting power dynamics in a completely new and more anarchic domain throw previous power structures into disarray. States cannot afford to ignore the implications of cyberspace dealings as it includes important infrastructures and hosts mass amounts of sensitive information. They must bolster their cybersecurity and allocate resources to ensure it is done sustainably. With different states adopting different cyber postures, it sets the stage for new power dynamic in a sphere that has no territorial boundaries as we know them. With this, cyber diplomacy and cyber diplomatic policies become more important than ever to define boundaries, severity of attacks, and how to properly assign attribution. The anarchic quality of cyberspace also levels out the previous playing field of international politics as states engage in a race for more advanced infrastructure and cybersecurity. This means that new power dynamics may emerge and supersede previous ones.

REFERENCES

Alasmari, A. (2021). Key role of diplomacy in promoting international cybersecurity: A case study of kingdom of Saudi Arabia (Order No. 28412401), Dissertation Thesis. Available from ProQuest Central. (2522839228). Available at: <https://login.proxy038.nclive.org/login?url=https://www.proquest.com/dissertations-theses/key-role-diplomacy-promoting-international/docview/2522839228/se-2>.

Alhammadi, A. (2021). The neorealism and neoliberalism behind international relations during COVID-19, World Affairs, 185(1), 147-175. DOI: 10.1177/00438200211065128

Attatfa, A., Renaud, K. & De Paoli, S. (2020). Cyber diplomacy: A systematic literature review, Procedia Computer Science, 176, 60-69. DOI: 10.1016/j.procs.2020.08.007

Barrinha, A. & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace, International Affairs, 96(3), 749-766. DOI:10.1093/ia/iiz274

Bendiek, A. (2018). The EU as a force for peace in international cyber diplomacy, SWP Comment, (19/2018), 1-8. Available at: <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-57428-2>.

Bodoni, C. (2020). Applications of Digital Diplomacy in International Organizations. In Cîrciumaru, F. & Bogzeanu, C. (eds.), Proceedings of the International Scientific Conference Strategies XXI, The Complex and Dynamic, Nature of The Security Environment, vol. 1. (pp. 213-218). Centre for Defence and Security Strategies Studies, "Carol I" National Defence University.

Calleri, M. (2020). The European Union as a global actor in cyberspace: Can the cyber sanctions regime effectively deter cyber-threats?, Romanian Cyber Security Journal, 2(2), 3-9. Available at: <https://rocys.ici.ro/documents/fall2020/article_1.pdf>.

Djedei, A. & Salim, K. (2021). The multi-dimensional impact of the pandemic on Sino-American relations: A neo-realist perspective, International Journal of Legal and Political Research, 5(3), 11-34.

Donaldson, S. E., Siegel, S. G., Williams, C. K. & Aslam, A. (eds.) (2015). Cybersecurity frameworks. Enterprise Cybersecurity, Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats, 1st ed., 297-309. Apress, Berkeley, CA.

Fantin, S. (2019). Privacy and cybersecurity in Europe: Policy, legislation and opportunities. Available at: <https://library.naist.jp:19943/dspace/handle/10061/13997>.

French Government Ministries. (2017). French White Paper on Defence and National Security. Available at: <https://issat.dcaf.ch/Learn/SSR-Methodology-Guidance/SSR-Thematic-and-Sectoral-Guidance/Defence-Sector-Reform-Guidance/French-White-Paper-on-Defence-and-National-Security>.

Goldman, E. O. (2020). From reaction to action: Adopting a competitive posture in cyber diplomacy, Texas National Security Review, 3(4), 85-101.

Goldman, E. O. (2021). Cyber Diplomacy for Strategic Competition, The Foreign Service Journal. Available at: <https://afsa.org/cyber-diplomacy-strategic-competition>.

Goolsby, R. (2019). Developing a new approach to cyber diplomacy: Addressing malign information maneuvers in cyberspace. In Lochard, I. V. (ed.), Senior Leadership Roundtable on Military and Defence Aspects of Border Security in South East Europe, 105-116. DOI: 10.3233/978-1-61499-908-9-105

Kurowska, X. & Reshetnikov, A. (2018). Russia's trolling complex at home and abroad. In Popescu, N. & Secrieru, S. (eds.), Hacks, Leaks and Disruptions: Russian Cyber Strategies, 25-32. European Union Institute for Security Studies (EUISS). Available at: <http://www.jstor.org/stable/resrep21140.6>.

Lancelot, J. F. (2020). Cyber-diplomacy: cyberwarfare and the rules of engagement, Journal of Cyber Security Technology, 4(4), 240-254 DOI :10.1080/23742917.2020.1798155

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia, Australian Journal of International Affairs, 75(4), 432-459. DOI: 10.1080/10357718.2021.1926423

Manantan, M. B. F. (2021). Defining cyber diplomacy. Australian Institute of International Affairs. Available at: <https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/>.

Minchev, Z. (2021). Disruptive effects of new pandemic age to shifted cyber diplomacy due to multilateral mixed transformation, International Journal of Cyber Diplomacy, 49-59. Available at: <https://ijcd.ici.ro/documents/2021/IJCD-art4.pdf>.

Pavel, T. (2020). Israel's cyber diplomacy - Looking for Israel's cyber ambassador, Diplomacy & Intelligence / Revistă de Științe Sociale, Diplomație și Studii de Securitate, 14, 208-216. Available at: <https://www.ceeol.com/search/article-detail?id=879290>.

Popescu, N. & Secrieru, S. (2018). Introduction: Russia's cyber prowess - where, how and what for?. In Popescu, N. & Secrieru, S. (eds.), Hacks, Leaks and Disruptions: Russian Cyber Strategies, 9-12. European Union Institute for Security Studies (EUISS). Available at: <http://www.jstor.org/stable/resrep21140.4>.

Sarcinschi, A. (2020). Potential new sources of power in international politics case study: COVID-19 pandemic and health resources. In Cîrciumaru, F. & Potîrniche, M. (eds.), Proceedings of the International Scientific Conference Strategies XXI, The Complex and Dynamic, Nature of The Security Environment, 114-123. Centre for Defence and Security Strategies Studies, "Carol I" National Defence University.

Soldatov, A. & Borogan, I. (2018). Russia's approach to cyber: The best defence is a good offence. In Popescu, N. & Secrieru, S. (eds.), Hacks, Leaks and Disruptions: Russian Cyber Strategies, 15-24. European Union Institute for Security Studies (EUISS). Available at: <http://www.jstor.org/stable/resrep21140.5>.

Torres, M. & Riordan, S. (2020). The cyber diplomacy of constructing norms in cyberspace, G20 Insights: Multilateralism and Global Governance. Available at: <https://www.g20-insights.org/wp-content/uploads/2020/12/the-cyber-diplomacy-of-constructing-norms-in-cyberspace-1607613238.pdf>.

Solana AQUINO

Is a graduate student at the University of the Philippines, Diliman Department of Political Science studying International Studies. She graduated BA Psychology with Latin Honours at the same university. Her research focus is on cyber diplomacy and cybersecurity.