Regulating Big Tech: Directions for a European Common Foreign Policy on Technological Diplomacy

Thesis Presented for the Master of International Relations - Global Order in Historical Perspectives

Under the supervision of Dr. J. Fynn-Paul

Nathan van der Heyden

June 2019

Table of Contents

Terms and Definitions

It seems necessary to disambiguate a few terms and offer a proper definition to terminology both in the domain of technology and diplomacy before starting this thesis.

Digital Diplomacy refers to the different new methods of conducting diplomacy using new technologies. It is different from Techplomacy because it does not refer to diplomacy *with* tech companies but rather *by* using new technologies and means of communication.

Techplomacy (also called tech diplomacy) is a portmanteau of technology and diplomacy. It is used to refer to diplomatic interactions between tech companies and traditional actors such as governments.

Cyber diplomacy is used to refer to the security side of technological diplomacy, more precisely to cybersecurity concerns.

Cyber more generally can be used both as a noun and a prefix that refers to various digital or computer-related activities.

Big Tech is used to refer to companies based in Silicon Valley and elsewhere who are defined by a reliance on modern technology (internet, mobile, AI, big data…) in their business offering.

Abstract

This thesis will underline the ongoing changes in European Foreign Policy in the context of digital diplomacy (ranging from cyber diplomacy to techplomacy) and will provide options

for further cooperation with technological companies from Silicon Valley, often referred to as Big Tech. First, I will argue that there is currently a diplomatic deficit created by the lack of diplomatic interaction between traditional actors and the new powerful non-state actors that are Big Tech. Second, I will observe the current means, objectives and actions the EU is deploying to interact with these companies and analyse the benefits and effectiveness of its strategy. Finally, I will provide recommendations, based on currently existing models of representation and means of communication between state and non-state actors, to improve the EU's reach and influence in Silicon Valley

Introduction

The academic debate around the impact of Big Tech has shifted in the last five years, as their public profile was taking a notable hit following a host of scandals hurting privacy and democracy. In a 2017 paper, Joshua Tucker and his colleagues demonstrated this change by pointing to the TIME Person of the Year in the last decade. In 2010, Zuckerberg won the award and was credited for turning the internet into a "friendly world, a serendipitous world"[1] . In 2011, it was the protesters of the Arab Spring, organising often through social media, who took the award. In 2017, it was Donald Trump who quickly took to his social media of choice, Twitter, to thank the TIME staff for this honor. This was particularly controversial as the role of social media through his campaign had been particularly problematic with many allegations of Russian meddling in the 2016 US election. Tucker and his colleagues write: "In other words, in only five years social media have gone—in the popular imagination at least—from being a way for prodemocratic forces to fight autocrats to being a tool of outside actors who want to attack democracies."[2]

Politics is not the only domain which has seen a greater influence of social media. As Robert Gorwa argues, virtually all aspects of our modern lives have endured the ubiquitous influence

[1] Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of Democracy*, *28*(4), p.46. doi:10.1353/jod.2017.0064
[2] Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of Democracy*, *28*(4), p.47. doi:10.1353/jod.2017.0064

of Big Tech[3]. The dangers of these companies intertwined so closely with our daily lives are described perhaps nowhere so poignantly than in Shoshana Zuboff's recent book: "The Age Of Surveillance Capitalism". According to her, the economic logic of capitalism, boosted by the advent of new technology and, in particular, Big Data analytics, has lead to the increasing commodification of things that were not part of the economic sphere previously. With the advent of surveillance capitalism, it is human experience itself that is commodified. Through this process, companies try to better predict human behaviours to anticipate market needs and, Zuboff argues, this approach culminates in actually controlling human behaviour, compromising any form of agency[4].

While this thesis will not attempt to describe the consequences of social media and other Big Tech companies on human lives, understanding that there are very good reasons for attempting to direct these companies towards beneficial effects for the general public is key. What is undeniable is that Big Tech companies are becoming increasingly powerful and, as their power grows, states slowly lose theirs. In a recent paper, Donaldson and Younane Council described this diffusion of power from states to non state actors as creating a diplomatic deficit[5]. The international community is simply not properly tooled diplomatically to reach out to these new powerful actors and, as Carne Ross already argued in the 2007 "Independent Diplomat: Dispatches From An Unaccountable Elite": the current diplomatic system is no longer adapted to the realities of the world. In the last 13 years, this has not changed. Problems are increasingly transnational, from climate change to terrorism but also migrations, cyberwarfare and many more. Not only single countries have become powerless facing these issues, but the authors argues that "The state system itself with its formalised diplomacy, dominant since the Treaty of Westphalia in 1648, may no longer be sufficient to resolve today's global challenges"[6].

[3]

[4]Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.

[5]Donaldson, A., & Younane, I. (2018, February). A diplomatic deficit? The rise of non-state actors. Retrieved from https://www.britishcouncil.org/research-policy-insight/insight-articles/diplomatic-deficit-actors

[6]Donaldson, A., & Younane, I. (2018, February). A diplomatic deficit? The rise of non-state actors. Retrieved from https://www.britishcouncil.org/research-policy-insight/insight-articles/diplomatic-deficit-actors

This thesis will argue that this diplomatic deficit should be a trigger for the European Union to treat the growing power of Big Tech as an important opportunity. As this thesis will show, certain individual member states have understood this and updated their foreign policy to both take full advantage of the potential of Big Tech and potentially steer it in a direction that is beneficial for their citizens. This thesis will argue that it is crucial for the EU to build on this trend and develop a coherent common foreign policy around Big Tech.

This raises two major academic debates. First, while certain scholars believe that a common foreign policy (CFP) is unrealistic for the EU, others think they are in a perfect position to spearhead the regulation cyberspace in cooperation with Big Tech. Expert in European Studies Dieter Mahncke argues that the creation of a CFP could prove problematic for the EU due to the fact that the bigger member-states would have to give up their comparative advantages to their neighbours to agree to a common diplomatic representation in Silicon Valley. Many member-states already have well-functioning diplomatic representation in the area and count on these to take advantage of technological innovation before their neighbours [7]. However, Patryk Pawlak, the executive officer for the European Union Institute for Security Studies argues that the potential benefits of a CFP outweigh the starting loss of influence and that the EU, as a supranational organisation, is at the right level to do what member-states alone do not have the political weight to do. According to Pawlak, acting and negotiating with the full weight of the common market will allow member-states a much bigger say in the direction of technological innovation then they could ever hope to achieve alone[8].

The second debate revolves around the very desirability of closer cooperation between Big Tech and democratically elected representatives. Gorwa argues for example that there is a risk associated in inviting these companies to the negotiating table. Not only does it dilute political power from the hand of the public, but companies could also use this opportunity to improve their image. As he notes: “Both politicians and the public should be mindful of portraying tech firms and states as equal partners, and transferring diplomatic metaphors to

[7] Mahncke, D. (2014). A post-modern foreign policy. *New Approaches to EU Foreign Policy*, 163-177. doi:10.4324/9781315771151-9

[8] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.168

the public-private realm. This imagery may be more helpful to Big Tech's public relations efforts than to crafting sound public policy."[9]. While keeping this worry in mind, a comparison between two meetings between the social media giant Facebook and European politicians will demonstrate why cooperation with the tech giants is more likely to bear fruits than a confrontational strategy.

On March 22 2018, CEO of Facebook Mark Zuckerberg left the European Parliament after having spent little more than an hour avoiding the tricky questions of European lawmakers. This long awaited hearing had been thoroughly negotiated beforehand by Facebook's legal team and the European Parliament had to agree to the terms set by the tech giant which saw the lawmakers ask questions for 45 minutes before Zuckerberg had a chance to answer but left no time for follow-up questions. The media was quick to point out that this had clearly been a failure from the EU. Politico claimed the European lawmakers were "outraged"[10] and reported that several key members of the European Parliament criticized the format, which was also the main criticism from The Guardian which described it as a "terrible way to elicit answers from one of the most powerful people in the world"[11].

A little more than a year later, French President Emmanuel Macron sat down for a meeting with Zuckerberg's team at the Elysée, in the very room in which he receives the heads-of-state of foreign countries. This change marks a widely documented evolution that the world of diplomacy and foreign policy must take into account. Big Tech companies have not only surpassed most of the world in terms of finance, population and power but their policy decisions now greatly influence the lives of millions. Gorwa argues that for the first meeting, Zuckerberg begrudgingly accepted to a hearing in Brussels after a committee tried "every trick in the book"[12] to get him in Brussels, and that he managed to name his conditions

[9] Gorwa, R., & Peez, A. (2019, June 27). Big tech hits the diplomatic circuit. Retrieved from https://berlinpolicyjournal.com/big-tech-hits-the-diplomatic-circuit/

[10] Cerulus, L. (2018, May 23). Mark Zuckerberg dodges punches at European Parliament. Retrieved from https://www.politico.eu/article/mark-zuckerberg-dodges-punches-at-european-parliament/

[11] Waterson, J. (2018, May 23). Five things we learned from Mark Zuckerberg's European Parliament appearance. Retrieved from https://www.theguardian.com/technology/2018/may/22/five-things-we-learned-from-mark-zuckerbergs-european-parliament-appearance

[12] Gorwa, R., & Peez, A. (2019, June 27). Big tech hits the diplomatic circuit. Retrieved from https://berlinpolicyjournal.com/big-tech-hits-the-diplomatic-circuit/

and the format of the hearing to be as favorable as possible. On the other hand, when Macron intelligently drew him to Paris "by threatening new legislation, but also dangled a carrot to match his stick."[13]. Macron gave Facebook the opportunity to participate in the creation of regulation around content on the social media to create a policy that worked for both of them.

The objective of this thesis is to first justify then propose a path for closer cooperation between the EU and Big Tech through technological diplomacy (Techplomacy). In the first chapter, this thesis will argue that there is an existing diplomatic deficit that is made even more apparent by the fact that tech companies are now acting as global actors. As long as diplomacy limits itself to the Westphalian model of international relations, they will both miss out on the opportunities that technological development bring and potentially suffer the consequences of their capitalist agendas.

In the second chapter, the focus will be on the necessary shift in mentality the EU has started to undertake in the domain of cyber security. Until recently, the EU focused on the risks of cyber warfare when it came to the dangers associated with the internet. Accordingly, when it comes to the internet and digital diplomacy, the European Union's Foreign Policy, also called Global Strategy, has been heavily centered around cyber diplomacy. It advocated multilateral partnerships to protect itself and its allies against state and non-state cyber attacks. Cybersecurity at that point was the sole area of focus when it comes to the internet.

Since 2018, in the aftermath of the Cambridge Analytica scandal and the claims that Russia had influenced the American elections through social media, the discourse has started to change. The 2018 Progress Report on the Global Strategy announces that the EU will protect itself from "malicious cyber activities that threaten the functioning of our democracies"[14]. EU policy adviser Antonio Missiroli considers that in the past few years, western countries have been struck by more cyber-enabled interference operations than ever. While some of these are traditional cyber attacks such as the one that hit the Organisation for the Prohibition of Chemical Weapons, or the ones which affected the Catalan referendum, the Brexit

[13] Gorwa, R., & Peez, A. (2019, June 27). Big tech hits the diplomatic circuit. Retrieved from https://berlinpolicyjournal.com/big-tech-hits-the-diplomatic-circuit/
[14]European External Action Service. (2018). The EU Global Strategy – Year 2, p.15.

referendum or the 2016 US presidential election were closer to propaganda, disinformation campaigns or "hack-and-leak" operations[15].

This paradigm shift is articulated by Powers and Jablonski in their book "The Real Cyber War". The authors argue that discourse over the role of the internet in society and international relations has been focused around cybersecurity, simply transporting military strategy and conflict into the digital realm. However, they argue that this is heavily underestimating the power of the internet. Their definition for the cyberwar encompasses "the variety of ways the internet is used to further a state's economic and military agendas"[16]. Considering how the internet shapes political discourse, cultural and social interactions, economical consumption etc., it seems foolish to only approach internet policy making from a military strategic point of view. According to them, the cyberwar is above all an information war that started with the invention of the postal service. Since then: "states have been preoccupied with how to leverage information systems for political, economic, and social power."[17]

Without downplaying the potential damage of cyber attacks, techplomacy underlines the need to consider the whole range of threats of the digital world. Some of these new threats exist because so many citizens are now using incredibly popular services provided by giant companies such as Google, Facebook or Amazon. To properly position itself in this new cyberwar, Jablonski and Powers argue that states (or, as this thesis will argue, the EU) should position themselves intelligently and cooperate with all the powerful actors in this complex system.

If the assumption of the first chapter is correct and a diplomatic deficit does exist in which Big Tech does have a global agenda and is left out of traditional diplomacy, then there is a need for techplomacy. The third chapter will offer an account of the different ways in which european countries attempt to secure influence in Silicon Valley and propose potential ways

[15] Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *24*(2), 135-153.
[16] Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press,. p.2.
[17] Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press,. p.7.

in which the EU could build on their existing initiatives for cooperation. In a recent paper in the Hague Journal of Diplomacy, the world's first Tech Ambassador for the country of Denmark justified his position by arguing that "the speed of emerging technologies and massive influence of multinational tech companies challenge traditional governance structures and diplomatic services around the world"[18]. Technological innovation has pushed Denmark to adapt and update their diplomatic relations to a changing global structure of international relations and the EU should follow this lead considering that, as Klynge argues: "the multinational tech companies driving this technological innovation have become extremely influential; to the extent that their economic and political power match — or even surpass — that of our traditional partners, the nation states"[19].

Chapter 1: The Rise of Tech Companies as Global Actors

Introduction

To properly tackle what Powers and Jablonski call "The Real Cyber War", it is necessary to challenge the classical scope of foreign policy and digital diplomacy. On the one hand, foreign policy is described as states influencing other states to further their own interests. On the other, digital diplomacy is often centered around cybersecurity and states often underestimate their interests regarding the internet, to a simple continuation of military strategy and conflict in the digital realm.

Many academics argue that changing both these conceptions is necessary[20]. This chapter will argue that this shift will not only benefit the Union's short and long term objectives, but is

[18] Klynge, C., Ekman, M., & Waedegaard, N. J. (2020). Diplomacy in the digital age: Lessons from Denmark's TechPlomacy initiative. *The Hague Journal of Diplomacy*, *15*(1-2), 185-195. doi:10.1163/1871191x-15101094
[19] Klynge, C., Ekman, M., & Waedegaard, N. J. (2020). Diplomacy in the digital age: Lessons from Denmark's TechPlomacy initiative. *The Hague Journal of Diplomacy*, *15*(1-2), 185-195. doi:10.1163/1871191x-15101094
[20] Donaldson, A., & Younane, I. (2018, February). A diplomatic deficit? The rise of non-state actors. Retrieved from https://www.britishcouncil.org/research-policy-insight/insight-articles/diplomatic-deficit-actors

also necessary and urgent. The EU's foreign policy has to encompass Big Tech for two reasons. First, as noted by Gorwa, tech companies have a massive impact on society, the global economy and geopolitical concerns[21]. Second, because these companies' international marketing strategies are already foreign policies themselves. They have serious economical power, often have more users than any country has citizens and they have short and long term interests that they're actively pursuing, including by influencing states[22].

Is Data the New Oil ?

In March 2017, The Economist published an article called "The world's most valuable resource is no longer oil, but data". Since then, this quote has been used by many and often changed to "data is the new oil" by newspapers such as the New York Times[23], The Economist[24] and Wired[25]. However, that metaphor is not quite right.

First of all, data is not a commodity in the sense that there is an easy market to buy and sell data. In the comparison to oil, data is more like crude oil, it cannot be sold as such but can be used by its producer, here, the service on which the data was generated, to produce valuable outputs : most typically targeted advertising that other companies will pay to have displayed to the right subset of users of the service. "Crude data" in itself is worth nothing but once "refined", it becomes the main revenue source of many services that consumers can use for free, simply because that usage is both the source of them producing data and the channel in which to display the target ads based on that data[26].

Second, data is not found underground but generated constantly by all of us. This does not, however, entail our data should be ours, considering we generate it voluntarily by using

[21] Gorwa, R. (2019). What is Platform Governance? Information, Communication & Society, 22(2019), 854-871.
[22] Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press,. p.9.
[23] Dance, G., LaForgia, M., & Confessore, N. (2018, December 18). As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. *The New York Times*.
[24] The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data. *The Economist*.
[25] Matsakis, L. (2019, February 15). The WIRED Guide to Your Personal Data (and Who Is Using It). *WIRED*.
[26] Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press,. p.76.

products that are often very hard to develop and expensive to maintain. If Google Maps uses my data and everyone else's in my area to better predict which route will bring me to my destination as fast as possible, I'm still choosing voluntarily to use this service for its convenience.

The true power of data is found in its ability to predict human behaviour. From policy effectiveness to marketing of consumer goods, understanding data is key to modern economics. As Powers and Jablonski note: "The predictive potential of big data is especially valuable, as it can help to more effectively market consumer goods and public policies."[27]

In light of this situation, data privacy and data rights have been at the center of a large debate in recent years. In this domain, the EU has taken a major step recently by introducing the controversial General Data Protection Regulation.

GDPR consolidates and unifies a fragmented and complicated network of national regulations from multiple member states. This provides clarity to the market, as well as a good set of teeth to the newly appointed European Data Protection Board, which will be able to punish companies breaching its provisions. However, some scholars find that the constraints of this regulation seem to misjudge the scale and the changes that Big Data brings about. These scholars argue that legislation of this sort - which is destined to guide the EU for the next decade - are unrealistic considering the fast-changing environment of this field. For them, much of the GDPR will soon be condemned to irrelevance.

There are two main positions in the academic debate on the GDPR. First, while some scholars argue that the GDPR will create more harmonisation amongst the European and by extension the global market[28], others argue that its effectiveness is hindered by the fact that significant parts of legislation are left to the national courts of the Member-States[29]. However, Albrecht argues that the previous legislation, the 1995 Data Protection Directive was both

[27] Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press,. p.76.
[28] Albrecht, J. (2016). How the GDPR Will Change the World. *European Data Protection Law Review*, *2*(3), p.287.
[29] Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, *47*(4), p.997.

outdated and more importantly, a directive only. This made it non-binding to member states and brought about the chaos in data protection regulation in the European Market. So for this reason, a common regulation is certainly a step in the right direction for the EU in terms of harmonization.

The second debate around the GDPR is more relevant to this thesis and encapsulates the high risk, high reward nature of technological development in Silicon Valley. Ideally, the effect of GDPR could apply beyond the European borders : global businesses would comply at global scale to the strictest of all the regional regulations - here GDPR - for two reasons. First, the high cost of having to comply with different standards of regulation, essentially necessitating the development of two different products would force businesses to comply with the stricter regulation to avoid waste. Second, ideally for the GDPR, the American public would not react well to the idea that American companies would be taking greater care of European customers data than theirs, prompting companies to adapt everywhere to GDPR-standards to avoid public and media backlash. The effects of the GDPR would then become global[30].

But some authors such as Zarsky believe that such a global effect is unrealistic. The most likely post-GDPR scenario, according to Zarsky, is that the growing nationalist tendencies of countries in the West would signify very little international pushback against different types of regulations in different countries[31]. Furthermore, the regulatory hurdles in the development of Big Data analytics would probably simply discourage both European innovation in this field and incentive for American companies to develop a product tailored to this market. Considering that in Big Data analytics, data is literally the source of income, we can almost disregard the size of the European market as a factor of economical bait if the regulations don't allow its use or conservation.

When regulations on Big Data analytics are developed, special care has to be taken considering the potential that this technology offers. A balance has to be struck between the privacy of users and the potential of the technology. While some like Albrecht argue that harmonisation of legislation will encourage Big Data practices, it seems much more likely

[30] Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, *47*(4), p.1018.
[31] Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, *47*(4), p.1019.

that this regulation will deter companies from exploring some of the more debatable applications of this very important technology. As Zarsky notes, even though the position of the EU on data privacy is admirable, it could also be strongly underestimating the potential future benefits[32].

Certain commentators also notably point out that this kind of legislation favors big companies. In "The High Costs of GDPR Compliance" journalist Chris Babel argues that Google or Amazon will have a much easier time ensuring their users' consent to their data being used than smaller companies who might struggle projecting trustworthiness to their users. Their larger legal teams will also allow them to adapt to (or circumvent) the regulation more easily, resulting in a risk of market domination by a few major companies and a cost of entry, both financial and of exposure, too high to create healthy competition. Babel reports that "83% of US privacy professionals expect GDPR spending to be at least $100,000"[33] and 40% of companies have estimated that GDPR compliance will cost them north of $500,000..

The above issues highlight how strong regulations can be dangerous in dealing with technological innovation and why the EU has to create a better strategy, which would include constant dialogue with the industry, especially during the development of new products. To take the example medical records data. Using artificial intelligence and machine learning, we can better predict on the basis of medical records how to treat future patients. The more complete the data is, the better AI can predict and find new solutions. However, more complete data also means less privacy for patients. A fine balance has to be found.

International Marketing Strategy or Foreign Policy?

Five major companies in Silicon Valley are often referred to as the Big 5 (or the GAFAM) : Google, Apple, Facebook, Amazon and Microsoft. There is great incentive for the EU to influence the decisions of these companies whose policy decisions affect the lives of millions.

[32] Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, *47*(4), p.1020.
[33] Babel, C. (2020, May 7). The high costs of GDPR compliance. Retrieved from https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263?

Apple[34] and Microsoft[35] are both valued right now at over $1 trillion according to data on ycharts. This is enough to rank them 17th compared to entire countries GDP; behind Mexico but ahead of Indonesia, the Netherlands or Saudi Arabia[36]. Facebook has more monthly users than any country in the world has citizens.

"The Real Cyber War: The Political Economy of Internet Freedom" explains well why the internet industry, data, and these tech companies are of the utmost importance for the future of the world. The authors argue that, while we think of cyberwar as viruses sent by hackers from foreign countries, what the authors call the real cyberwar has to do mostly with ideas and information[37]. The real cyber war as they describe it represents all the means a state uses on the internet to further its economic, strategic and military interests. This does obviously take into account the importance of coordinated cyber-attacks but too often these are overestimated compared to other means of influence and soft power. Whether it be leveraging information for political, cultural and economic gains; shaping political discourse and opinions or even societal values: that is where the greatest potential lies[38]. This is why the European Union needs to focus its resources to make sure that "the internet" stands for the same values it does. Moreover, the infrastructure supporting the internet and the cloud are mostly built in the United States, adding another reason to invest politically and diplomatically in the region.

The book argues that if geopolitics describes the "strategic actions taken by states to preserve their own national interests in an anarchical world"[39], too little research has been done on the potential of information technology and the internet to do exactly that.

[34]Apple Market Cap | AAPL. (2019, October 14). Retrieved October 14, 2019, from https://ycharts.com/companies/AAPL/market_cap
[35]Microsoft Market Cap | MSFT. (2019, October 14). Retrieved October 14, 2019, from https://ycharts.com/companies/MSFT/market_cap
[36]World GDP Ranking 2019. (2018, April 2). Retrieved October 14, 2019, from http://statisticstimes.com/economy/projected-world-gdp-ranking.php
[37] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.2.
[38] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.12.
[39] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.4.

Google's mission, as described by the company itself, is to "organize the world's information and make it universally accessible and useful". Its business model is deceptively simple. Offering great services and allowing access to more information than anybody fifty years ago could have dreamed of, all of that, for free. In exchange, Google simply harvests the data generated by all users of its services, personally and as a group. This data is then used for several purposes, the most important of which being the creation of a profile around each of its users to allow targeting of ads which generate much better returns than traditional ads. However, to keep the engine running, Google must keep its search engine excellent and ahead of the competition to make sure their users keep using their products and ensure access to the data and a platform on which to advertise and generate revenue[40].

This means that Google has two missions to continue making money. First, they need to provide a great service to their users. Second, they need to connect these users to relevant advertisers. To get an idea of how successful Google is at this, suffice it to say that it generates more than 10 times the revenue than the next search engine (Yahoo!)[41]. The possibilities of what it can do with that data are also impressive. Eric Schmidt, ex-CEO of Google once explained that the data harvested by the search engine was capable of predicting the stock market - "but then we decided that it was illegal. So we stopped doing that."[42]. While advertising represents the vast majority of its revenue, the possibilities for Google going forward for alternate revenue streams are plentiful.

Google is also a major actor in emerging parts of the world. It supported the growth of the internet in various countries and continents including the Middle-East and is continuing to improve global connectivity even in rural areas with projects such as Project Loon, using balloons flying at twice the altitude of commercial aeroplanes to provide internet to large rural areas at decent speeds[43].

[40] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.77.
[41] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.79.
[42]"FY2011 Revenue by Geographic Segment," Cisco Systems Annual Financial Statements. Retreived October 12 2019 from http://investor.cisco.com/financialStatements.cfm.
[43] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.92.

To return to the comparison with oil, no company has ever dominated the oil market in the way Google dominates the information market. However, contrary not only to the oil market but to virtually any market, data is not taxed. If information is a commodity in the modern economy, many scholars argue that a good balance between taxing companies growing at alarming rates and fostering the development of technology must be struck by governments[44].

While Google's actions around the world often seem positive, the company's motto "don't be evil" is not the only driver of their actions. As noted in "The Real Cyber War", even though Google clearly supports freedom to connect and freedom of expression as fundamental human rights, it does not mean its pursuit of global connectivity is motivated only by those noble values[45].

In view of these explanations over the functioning of the tech giant, it is possible to argue that the reason Google decides to promote freedom of expression and right to connect is that it's entire business model is based on people using its free services. The author compares this process to car manufacturers in the US during the twentieth century encouraging the rise of the middle class; while the goal may be noble, the justification is economical[46].

A recent example of such interference by tech giants concerns Google and Cuba. Eric Schmidt and three other high ranking Google Executives travelled to Cuba in 2014 with tourist visas, planning to do non-commercial research. These travels led to business deals between Cuba and the tech giant, even though in 2014 Cuba was still under the American embargo that kept any other company for the last half of a century to do any business with the island. Since then, several new deals have flourished between the two culminating last March in a physical undersea cable linking Cuba to Google's network. Only six months after the first trip in 2014, the Obama administration lifted the embargo and eased restrictions on

[44] Hill, A. (2018, November 2). The global hunt to tax big tech. Retrieved from https://www.ft.com/content/79b56392-dde5-11e8-8f50-cbae5495d92b

[45] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.97.

[46] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.98.

commercial endeavours. This trip, however, gave Google a six month lead over its competitors to connect the island to the internet through their network[47].

It seems relatively clear that both parties had a lot to gain from such cooperation. On the one hand, the Obama administration could lay the diplomatic groundwork for further cooperation with Cuba without actually having to do so itself and on the other Google gained access to 10 million new potential users.

What is more worrisome, and highlights the need for greater control and oversight, is that this whole trip was planned by Google's philanthropic think tank Jigsaw. This think tank has been helmed since its inception by Jared Cohen, ex-State Department, highlighting the links between Google and the American government. Schmidt and Cohen met during an official trip to Iraq in 2009, after which Google helped the government launch its first Youtube channel[48].

Since then, from Cohen's own declaration, Google has been conducting diplomatic missions for the State Department where the situation wouldn't be very welcoming to the American government itself[49]. While many projects of Google have been very positive and supportive of human rights, Jablonski and Power's assessment that Google is essentially pursuing new markets through philanthropic projects is supported by the analysis of their philanthropic arm Jigsaw.

From Obama's own speech announcing the end of the embargo : "I believe in the free flow of information. Unfortunately, our sanctions on Cuba have denied Cubans access to technology that has empowered individuals around the globe."[50]. Google's interests are partly motivated

[47] Google's Diplomatic Edge. (2019, March 28). Retrieved from https://www.googletransparencyproject.org/articles/googles-diplomatic-edge.

[48] Google's Diplomatic Edge. (2019, March 28). Retrieved from https://www.googletransparencyproject.org/articles/googles-diplomatic-edge.

[49] Google Unveils Tools to Access Web From Repressive Countries. (2013, October 21). Retrieved from http://business.time.com/2013/10/21/google-digital-rebels/

[50] Scola, N. (2014, December 18). At the heart of Obama's Cuba doctrine? The Internet. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/at-the-heart-of-obamas-cuba-doctrine-the-internet/

by economic reasons and they are certainly influencing the political realities in many countries to ensure its own economic growth.

The controversial figure Julian Assange, the founder of Wikileaks, called Jared Cohen "Google's director of regime change"[51]. Further analysis of Google's Jigsaw led him to declare that "A don't be evil empire is still an empire". Google is, for a lot of the developing world in particular, becoming synonymous with the internet. However, we can't expect Google to be a disinterested agent for the common good, after all, as Schmidt himself noted in an interview with Brian Womack of Bloomberg in 2012: "It's called capitalism. We are proudly capitalistic. I'm not confused about this."

Google, and most of Big Tech, are undoubtedly using their influence to further their own interests in the world. In line with the earlier definition of foreign policy, these new non-state actors can dwarf economically and demographically certain states and this chapter has shown that their global agenda can be compared to a state's foreign policies.

This is what creates what Donaldson and Younane call a diplomatic deficit. They note that "Traditional state diplomacy conducted behind closed doors (...) risks perpetuating the self-interest of certain states and their diplomatic elites (...) failing to take advantage of the growing power of non-state actors (...) undermining the effectiveness of international diplomacy"[52]. This opinion is not unanimously shared as certain scholars point out that including companies in policy making has its own dangers. Gorwa for example points out that when Microsoft spearheaded the "Paris Call for Trust and Security in Cyberspace" announced at the 2018 Internet Governance Forum and demanded that, as the agreement reads "States must work together, but also collaborate with private-sector partners"[53], they omitted to point out their "own recent past of public-private interaction includes being the NSA's very first partner in the infamous PRISM surveillance program disclosed by Edward

[51] Assange, J. (n.d.). Google Is Not What It Seems. Retrieved from https://wikileaks.org/google-is-not-what-it-seems/

[52] Donaldson, A., & Younane, I. (2018, February). A diplomatic deficit? The rise of non-state actors. Retrieved from https://www.britishcouncil.org/research-policy-insight/insight-articles/diplomatic-deficit-actors

[53] Paris call for trust and security in cyberspace — Paris call. (2018, November 13). Retrieved from https://pariscall.international/en/

Snowden"[54]. Gorwa warns that the idea that opening the doors of cooperation would benefit the general public might be naive.

Global Agents of Change ?

Google is far from being the only company to seemingly externally promote positive values of human rights, freedom of speech and democracy. What is historically unique about it and the other tech giants is the power it has to influence the realities of millions. Companies such as Facebook were also heavily implicated in important geopolitical phenomenons such as elections, revolutions and protests around the globe.

In 2008, Facebook still in its infancy as a company and social network was used to organize protests against FARC in Colombia. Four million people rose up in Colombia and the rest of the world, marking the first massive political movement started, shared, marketed and planned for on social media[55]. The author Kirkpatrick argues in this same article that Facebook is the common thread in these protests, the Arab Spring, the events in Spain, India and Israel: Facebook, at first a social tool, is becoming the meeting hall of the world. A message of political nature can spread virally at a speed unimaginable before social media.

However this idea is heavily debated, with some arguing that social media is only one part of the equation, like Khamis, and others arguing that Facebook is not a tool for free speech. Mark Zuckerberg often brags that his social network is "giving everyone a voice" but the biggest social media might be better defined as an amplifier of the most dominant voices.

For Khamis, social media has certainly been a very important factor during the Arab Spring. However, she argues that "the will and determination of Arab people to implement change in their countries were the main driving forces behind the revolutions and uprisings"[56]. Of

[54] Gorwa, R. (2019). What is Platform Governance? Information, Communication & Society, 22(2019), 854-871.
[55] Kirkpatrick, D. (2011). Does Facebook have a foreign policy ? Foreign Affairs, 190. Retrieved from https://www.jstor.org/stable/pdf/41353271.pdf?refreqid=excelsior%3Ad5fed7e7771dbae069f2babfb6574d03
[56] Khamis, S. (2015). *Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies* (Doctoral dissertation, University of Maryland), p.21.

course, social media was certainly a catalyst, spreading news and greatly improving organisation. However, as another scholar argues : "technology does not cause political change but it does provide new capacities and impose new constraints on political actors"[57]. Briefly said, it is the political actors that provoke change, not their tools.

Evans even goes further in argumentation against the idea that social media is an agent of change and of freedom of expression. He argues that what we read on Facebook is what shows up in our News Feed and what shows up in our News Feed is what Facebook's algorithm decides should be in it[58].

Two forms of content are amplified by Facebook, first there is the native content, generated by users or by companies. For this native content, the algorithm promotes content users are most likely to interact and engage with, increasing the time spent on the website by users. The second content promoted is paid advertising. In both cases, the first one indirectly, the algorithm optimizes revenue[59].

Facebook also does not censor content based on veracity. Zuckerberg has stated Facebook will not censor political misinformation. The justification of this strange declaration was that he intends to keep Facebook's algorithm "content-agnostic". However, it is everything but that. The algorithm's job is to select which message or voice is the most likely to generate interaction and keep users interested[60].

Observing online behavior shows that optimizing for engagement is actually optimizing for outrage and polarization. Users of Facebook are more likely to interact with content they strongly disagree with than any other type. While Facebook believes that their algorithm being "content-agnostic" is the best way of staying neutral, this is completely invalidated by the fact that, in order to maximize revenue, their algorithm promotes content that is most

[57] Howard, P.N. (2011). The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam. Oxford: Oxford University Press, p.12.
[58]Facebook is not free speech, it's algorithmic amplification optimized for outrage – TechCrunch. (2019, October 20). Retrieved from https://techcrunch.com/2019/10/20/facebook-isnt-free-speech-its-algorithmic-amplification-optimized-for-outrage/
[59] Facebook is not free speech, it's algorithmic amplification optimized for outrage – TechCrunch. *op.cit.*
[60] Facebook is not free speech, it's algorithmic amplification optimized for outrage – TechCrunch. *op.cit.*

likely to create interaction. Since this second tenant is at the heart of their business model and their main source of revenue, it is very unlikely that this ever changes. According to Evans, while Facebook claims to be a voice for free speech, its capitalistic nature ensures that will never truly happen.[61]

Joshua Tucker and his colleagues point out that there has been a clear change in the public perception of social media and its impact on democracy. "Social-media technology is young, but has already played a part in numerous turbulent protests and a highly polarized U.S. election. Social media have often been described as the site for conflict between "good" democratic forces who use social media to make their voices heard and "bad" autocratic and repressive forces who aim to censor this channel to silence these liberal elements. However, recent worries that illiberal and extremist forces might use the freewheeling world of online communications to undermine democracy reversed the discussion about social media. After the 2016 U.S. election, even leaders of democracies called for greater "regulation" of the internet. In this, they echoed—to a degree at least—authoritarian rhetoric that promotes censorship and "public-opinion guidance."[62]. The idea that social media can have great political power use to be seen as a advantage for democracy. Scholars are much more cautious today and in a world where the President of the United States conducts foreign policy on Twitter for millions to see, it is likely that we have still not seen all of the consequences of social media on democracy.

Conclusion : Why should the EU care ?

It seems that the equivalency between oil and data is not as easy to establish as it seems. A more proper one would be to say that Google, Facebook, Microsoft, Apple, Amazon and the other tech giants are the data-fuelled utility providers of our century. The services they provide are crucial to our modern economy.

[61] Facebook is not free speech, it's algorithmic amplification optimized for outrage – TechCrunch. *op.cit.*
[62] Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. Journal of Democracy, 28(4), 46-59. doi:10.1353/jod.2017.0064

These companies are the infrastructure of our social, political, economic and cultural systems. What they provide is the medium for any discussion. While companies have always tried to sway politicians to influence legislation in their favor, these companies can shape political discourse more than any single entity ever could as it increasingly takes place online[63]. The Washington post reported that in 2017, Google had also spent more money than any other company to influence Washington. "All told, the search giant broke its own record by allocating more than $18 million to lobby Congress, federal agencies and the White House on issues such as immigration, tax reform, and antitrust."[64]

Even though they might promote free speech and democratic values, it has also been demonstrated earlier in this thesis that these values can hide economical considerations and that the promoted free speech often ends up by design being amplification of the extreme opinions. Moreover, seeing that these private companies have an enormous amount of influence on society means that they have a considerable amount of undemocratic power both over political issues but also over the global economy[65].

The question of this thesis is both why and how the EU should step up its diplomatic interactions with tech companies in Silicon Valley. While a strategy is already in place and actions are being taken, such as the GDPR, to protect citizens and their data, more can be done. Closer control and interaction has to be a priority for the EU with a heavy focus on protecting the political and economical spheres from the influence of these privately-owned, capitalistic companies.

Chapter 2: Defining EU Diplomacy Objectives

[63] Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. Journal of Democracy, 28(4), 46-59. doi:10.1353/jod.2017.0064

[64] Shaban, H. (2018, January 23). Google for the first time outspent every other company to influence Washington in 2017. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/01/23/google-outspent-every-other-company-on-federal-lobbying-in-2017/

[65] Powers, S., M. & Jablonski, M. (2015)*The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press, p.97.

Introduction

Technology transcends diplomacy. Like so many other spheres, economic, social and many more, diplomacy has evolved very quickly these last few years. New methods of conducting diplomacy have appeared with the internet, referred to, as a whole, by the term digital diplomacy. The core of diplomacy has always been information and communication. However, in "Digital Diplomacy: Theory and Practice", Bjola and Holmes argue that the internet has completely changed the way we provide, consume and share information and the tools that the internet can provide for communication are "nothing less than a revolution in the practice of diplomacy"[66].

The academic interest on digital diplomacy has been largely focused on one issue, namely the interaction between social media and public diplomacy. Obviously, the tools provided by the internet for public diplomacy are simply incredible. Considering public diplomacy is about influencing the public, the sheer reach of these tools is immense considering the popularity of social media. Most embassies now use social media platforms such as Twitter, Facebook or Instagram where they can create polls for their followers, organise and promote events. The other side of the coin is that governments can use trolls, bots and fake news to hinder support for certain measures or promote their own interests in foreign countries[67].

Bjola and Holmes argue that a fundamental aspect of diplomacy is to assess and manage change. Society changes constantly and assessing and adapting to these changes is crucial for a diplomat. It is undeniable that the innovations the internet has brought to diplomacy are surely an immense paradigm shift but it is interesting to remember Lord Palmerston's reaction, then the British Foreign Secretary, to receiving the first telegram in 1850 : "My God, this is the end of diplomacy!". Adapting to change has always been a fundamental part of diplomacy. According to them, diplomacy should be "a method of protecting the status quo by anticipating tensions and preventing them from unsettling the international order"[68].

[66] Bjola, C., & Holmes, M. (2015). *Digital Diplomacy: Theory and Practice*. London, England: Routledge, p.1
[67] Bjola, C., & Holmes, M. (2015). Digital Diplomacy: Theory and Practice. London, England: Routledge, p.9
[68] Bjola, C., & Holmes, M. (2015). *Digital Diplomacy: Theory and Practice*. London, England: Routledge, p.2.

This chapter will first discuss what the strategy of the European Union has been considering this technological change, what were their plans to protect from future tensions and how this plan has evolved in the past 4 years. Second, it will look into what the potential for EU diplomacy is in regards to Big Tech and whether the EU can create a common foreign policy regarding the internet. Third, this chapter will reflect on what the EU's policy guidelines concerning the internet should be. Finally, it will look at the potential of the danish model of techplomacy and see if such model could be adapted to the EU and the benefits it might have.

EU Global Strategy

The European Union has noticed the need for better management and adaptation to change when it comes to the internet. However, their focus has not always been on the wider implications that technological innovation and Big Tech can have on society. The 2016 Global strategy for the foreign and security policy of the European Union, EUGS for short, is the new and improved doctrine for EU foreign policy.

While the EUGS admits that the Union is not making full use of its potential when it comes to technology, it seems that this is an understatement. The section about technological innovation makes no mention whatsoever of Big Tech or even the internet for that matter[69]. Even though plans to "deepen our partnerships with civil society and the private sector as key players in a networked world"[70], no clearer explanation is given of what that could mean or how these partnerships could be implemented. The EUGS simply does not mention anything about technological innovation and the internet in its foreign policy plans for the foreseeable future that is not linked to protection against cyber attacks. Finally when the internet is mentioned, it is only to argue that the EU needs better tools to defend itself against cyber attacks guaranteeing access to data and computer systems in case of military conflict. The EU

[69] European External Action Service. (2016). *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy*, p.3-5.
[70] European External Action Service. (2016). *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy*, p.8.

is to defend itself by building stronger partnerships between member-states but also with the US and NATO.

Still in 2016, cyber security and cyber diplomacy were absolutely the name of the game for the EU when it came to digital diplomacy. As Powers and Jablonski argued in "The Real Cyber War", the shift from understanding the cyber war in strategic military terms to understanding it as any way an actor exerts influence using digital technology had not yet happened in EU foreign policy. The focus, in the EUGS and in the first progress report of 2017 was on "hybrid threats"[71], meaning military threats that could be both traditional and digital.

It seems however that the 2018 second report showed a greater interest in other forms of influencing over the internet and provided more information on the new types of foreign threats the EU was planning to prepare against. The timing of this is quite telling, as well as the terms used.

> *"The EU has accelerated its work on Cybersecurity, which is critical to both our prosperity and our security. Malicious cyber activities not only threaten our economies and the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Cyber threats come from both non-state and state actors: they are often criminal, motivated by profit, but they can also be political and strategic"*[72].

While the EU still considers this cyber security, it's not limited to military matters. The EU seems to consider seriously that the damage that can be done by "malicious cyber activities" is not only to digital infrastructures but also to "our democracies, our freedoms and our values". The document also vows to step up the fight against deliberate disinformation[73].

[71] European External Action Service. (2017). *The EU Global Strategy – Year 1*, p.5.
[72] European External Action Service. (2018). *The EU Global Strategy – Year 2*, p.15.
[73] European External Action Service. (2018). *The EU Global Strategy – Year 2*, p.16.

It seems that these new objectives are directly linked to the Facebook-Cambridge Analytica scandal of early 2018, that hurt the EU by helping both the Trump campaign in the 2016 election and the Leave vote in the Brexit referendum. In both these cases, it was not the digital infrastructure of the EU that was threatened but the very fabric of democracy which was attacked by these malicious cyber activities. Both these votes are thought to have been heavily affected by targeted ads on social media, Facebook more precisely. Those ads were targeted by harvesting the data of millions of users without their consent[74].

What is most baffling about this case is how little Europe's foreign policy towards companies like Facebook has changed in the fallout of this case. Brexit is certainly a major event in the history of the EU but it seems not much has changed in how the EU interacts with Big Tech. Even though this 2018 second progress report seems to outline the threat, apart from an announced "cyber diplomacy toolbox", no actual measures are advocated for in the foreign policy of the EU regarding Big Tech.

This cyber diplomacy toolbox declares that wrongful acts in the eyes of international law could give rise to common EU action. Furthermore, it could use restrictive measures against aggressors[75]. The approach still seems to be retroactive in the sense that once a wrongful act has been done, the EU will investigate *a posteriori* any violations and possibly impose sanctions.

From the 2019 progress report, the shift from cyber attacks to hybrid attacks on democracy becomes more dominant. It announces the creation of a multilateral forum that would allow better governance and regulations on the digital world and technological innovation, including artificial intelligence[76]. It is finally with this new document outlining a strategic agenda for the next five years that the EU seems to promote cooperation with Big Tech on issues in the digital world.

[74] Davies, Harry (December 11, 2015). "Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users". The Guardian.
[75]Council of the EU (2017). Cyber attacks: EU ready to respond with a range of measures, including sanctions.
[76] European External Action Service. (2019). *A New Strategy Agenda: 2019-2024*, p.21.

This multilateral forum created in 2018 is the Global Tech Panel: “Launched by High Representative Mogherini, the #GlobalTechPanel brings together leaders from the tech industry, the world of investment, and civil society. The aim of the Global Tech Panel is to foster new types of cooperation between diplomacy and technology to address challenges and threats but also to make innovation a true force for good in an increasingly more complex and connected world”[77] as indicated on the European External Action Service. This Global Tech Panel (GTP) aims to better understand the challenges and opportunities that technological innovation, Big Tech and the internet offer. The focus is heavily put on cooperation with the private sector. The first meeting took place in Brussels in June 2018.

Federica Mogherini, High Representative of the EU has declared after the meeting that “Our discussions in the Global Tech Panel so far have strengthened my conviction that a new conversation is needed between diplomacy and technology leaders on solving problems together". The shift in focus from cyber diplomacy focused on security and techplomacy seems to have materialized in the Union’s foreign policy plans. Additionally, partnerships and cooperation with Big Tech have been included. Industry leaders such as Bill Gates and Brad Smith (from Microsoft) have been included in the dialogue.

The main focuses of this Global Tech Panel are automated weaponry, artificial intelligence, climate change and the economic transition brought by automation[78]. Using new technologies to their full potential seem to be the new driving force behind this Global Tech Panel. While that is certainly a step in the right direction, the fruits of the GTP have not yet been particularly exciting. The only concrete project so far that has came from the GTP is the creation of an education program in Tunisia centered around digitisation.

In the 2019-2024 New Strategy Agenda, the EU prides itself on the 250 Tunisian tech entrepreneurs to be coached in 2019 by leading Silicon Valley mentors as part of a Global Tech Panel pilot initiative.

[77] About the Global Tech Panel. (2019, January 11). Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/50886/about-global-tech-panel_en

[78] About the Global Tech Panel. (2019, January 11). Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/50886/about-global-tech-panel_en

Building on Cyber Diplomacy

While this thesis argues for the necessity if a shift in paradigm from cyber diplomacy to techplomacy, this does not mean the former should be abandoned all together. The transition must be done building on cyber diplomacy rather than replacing it. As Antonio Missiroli argues in « The Dark Side of the Web: Cyber as a Threat », the number of cyber attacks has actually increased in the past few years and have come to the forefront of international security issues and mediatic coverage culminating in the failed 2018 infiltration attempt by the Russian military intelligence service of the Organisation for the Prohibition of Chemical Weapons. The attack was foiled by the Dutch intelligence services in association with their english colleagues and in this process these two recuperated information about other attacks by the Russians on many international targets including the World Anti-Doping Agency[79].

The EU expressed solidarity in an official statement with the countries affected and denounced Russia for its attempt to undermine international law. In December 2018, the EU's diplomatic service was itself the target of a hack-and-leak campaign. Over the past few years, many elections, governments and public agencies in Western countries have been targeted by these clearly politically motivated cyber attacks, rarely more spectacularly so than during the Brexit vote or the US presidential campaign. While the objective is large scale destabilisation of democratic processes, the means to do so vary and make these attacks particularly problematic in the context of international law. Affecting the outcome of an election can be done in many different ways, from hack-and-leak operations to vote counting manipulation through a campaign of propaganda and mass-disinformation, and while certain of these activities are strictly prohibited, others are gray areas[80].

This is the reason why techplomacy should be considered in the multilateral approach to a defense against these attacks. International law fails to properly characterize and punish cyber

[79] Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *2019*(2), p.136.
[80] Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *2019*(2), p.137.

attacks because of their diverse nature that can't easily fit the definition of « armed attack ». Nevertheless, Missiroli warns that cyberattacks represent an excellent way of inflicting high-impact low-cost damage in a way that is difficult to deter and even detect. Simultaneously, the technological advances in Internet of Things technology (web-connected objects) and AI are creating new battlefields constantly and civil-society vulnerabilities. This creates a blurring of the nature of these attacks and of the international legal framework that is supposed to legislate aggression between nations. Some attacks could be classified as intelligence-gathering activities while others might threaten lives, goods or infrastructure. While international law doesn't explicitly prohibit espionage, it qualifies sabotage as a potential casus belli but cyberattacks are difficult to neatly fit in a specific box and attribute to a specific actor[81]. As Missiroli notes, further complications arise because of the impossibility to use classic arms control arrangements "as verification of stockpiles would be virtually impossible and compliance hardly enforceable: cyber assets and capabilities can be quickly recreated and, at any rate, the quintessential ubiquity and dual-use nature of information technology would make inspections pointless"[82].

These factors combined with the blurring of the relevant jurisdictions inherent to such attacks highlights the necessity of international public and private cooperation. Very often, these attacks cross multiple jurisdictions, they can be directed at a specific company in a country and still have international repercussions as was seen in the attack hitting the world's biggest sea-transport company Maersk in Denmark in 2018. This attack had been destined originally for Ukraine and the collateral damage to the Danish economy was a clear sign that more digital cooperation was needed.

This two-sided blurring is what justifies the increasing need for multilateral cooperation in order to create the most robust line of defense against cyberattacks: deterrence. Cold War doctrine type of deterrence does not apply to cyberattacks as the actors often include non-states and the barrier of entry is very low. The best way to create deterrence in this case is to build resilience, Missiroli argues. To do so, countries must cooperate and exchange

[81] Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *2019*(2), p.141.
[82] Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *2019*(2), p.145.

notes with their allies to ensure they stay on top of potential attacks and can detect them as in the case of the hacking of the OPCW. Governments must as well cooperate with private companies, whether they be tech giants or cybersecurity firms, to ensure that they stay one step ahead of potential hackers. As Missiroli writes: « Cybersecurity is a team sport and cooperation is essential »[83].

There are ways to enhance cybersecurity and reduce the power and frequency of cyberattacks through resilience that comes from cooperation and cyber diplomacy, but it is imperative to include private companies in this discussion as they operate the internet and represent massive amount of civilian traffic. Furthermore, the technological innovation that these companies are responsible for open new battlefields and vulnerabilities. This requires cooperation between the public and private sphere to make sure that civil society is adequately protected[84]. This is the reason why governments must improve their current cyber diplomacy by building on it with techplomacy rather than replacing it altogether.

Defining a Common Digital Foreign Policy

In the words of Louis Michel, at the time the Development Commissioner : "Together we can truly shape a more just and equitable world, and thus influence the fate of the world. And because we can, we must."[85]. This sentiment is what should guide the European Union in its common foreign policy. While the EU seems to have understood what it needs to do, it still has not had the potential impact it could have.

Explaining why is the subject of an academic debate centered around two main problems. In general, there seems to be very little European commonality in foreign policy. While certain scholars do not believe the EU even has the necessary tools to reach a Common Foreign

[83] Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *2019*(2), p.145.
[84] Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *2019*(2), p.147.
[85] European Commission - Louis Michel - Press Release, Bruxelles, (2006). Retrieved from https://europa.eu/rapid/press-release_SPEECH-06-689_fr.htm

Policy (CFP), it seems more likely that the reluctance from member states to agree on a CFP stems from other phenomenons.

At the heart of it, argues Dieter Mankhe, is the reluctance of member states to grant that authority to the Union. If the EU wants to make a difference globally it first must secure the backing of member states. Simply put, any CFP will imply setting aside specific national interests. He argues that there's not enough of a threat or potential benefit for member states to put their personal interests aside and band together for greater impact[86]. As of now, the biggest calls and potential drivers for a foreign policy are a common energy policy, common action for the climate or a common policy in the Middle-East. Right now, none of these are the object of truly common European policies.

Member states still seem to be too tightly attached to their own national identities and interests. Even though more than half the foreign investment in Silicon Valley comes from EU countries[87], this investment is fractured and is not providing the EU with the leverage it should have. Mankhe argues that divergences in foreign policy have hurt the EU in the past, different policies in Iraq had a devastating effect and still today, not all EU countries recognize Kosovo independence.

However, powerful member states have shown in the past to be capable of setting aside their comparative advantage to create a common economic policy. Mankhe argues however that the instigation of the Euro benefited both from a more hopeful popular outlook on Europe at the time and more rapid and attribuable results than a common foreign policy could deliver. In the case of a CFP, the need for it does not appear as pressing and the dominant actors are not willing to sacrifice their national interests for long term gains[88].

[86] Mahncke, D. (2014). A post-modern foreign policy. *New Approaches to EU Foreign Policy*, 163-177. doi:10.4324/9781315771151-9
[87] DiploFoundation. (2018). *The Rise of TechPlomacy in the Bay Area*.
[88]Mahncke, D. (2014). A post-modern foreign policy. *New Approaches to EU Foreign Policy*, 163-177. doi:10.4324/9781315771151-9

Achieving the EU's potential

A common foreign policy is only realistic for the EU if member states care about other member states problems as if it were their own. Spain has to care about Russia as much as the Baltics and Lithuania has to care about immigration as much as Greece. That is what Mankhe argues, highlighting the need for the EU to transcend nationality[89]. This is debatable for two reasons.

Where the divisiness of the EU can be understood as a weakness, some scholars argue that this is the EU's strength. Cross argues that it is actually the plurality of Europe that inspires and gives it a reputation as a "smart power". He argues that the General Strategy both proposes short term realistic goals and idealistic unreachable targets that the EU has to aim for, both together resulting in a doctrine of principled pragmatism. It is only because this idealism, these principles that the EU manages to create the necessary political will behind any common foreign policy[90]. In other words, Spain does not have to care about Russia as much as the Baltic States, but Spain has to care about european idealism.

Second, not all common foreign policy issues are tied to geographical concerns. Climate change, while it does not affect all european countries equally still concerns all of Europe. The internet is the perfect example, all countries are potentially threatened by cyber attacks or other malicious cyber activities, giving them ample cause for a common foreign policy concerning the web.

Certain scholars, such as Michael Smith, argue that the EU is incapable of achieving what it sets out to do in the General Strategy. They argue that there is simply not the necessary treaties and potential in place for the EU to create a common foreign policy[91]. However, a closer look at official EU documents shows that this is not the case. The creation in 2010 of

[89]Mahncke, D. (2014). A post-modern foreign policy. *New Approaches to EU Foreign Policy*, 163-177. doi:10.4324/9781315771151-9

[90]Cross, M. K. (2016, October 10). The EU Global Strategy and diplomacy. Retrieved from https://www.tandfonline.com/doi/full/10.1080/13523260.2016.1237820

[91] Smith, M. E. (2016). Implementing the Global Strategy where it matters most: the EU's credibility deficit and the European neighbourhood. *Contemporary Security Policy*, *37*(3), 446-460. doi:10.1080/13523260.2016.1240467

the European External Action Service (EEAS) following the Treaty of Lisbon and the appointment of the High Representative should give the necessary weight to the EU to create a common foreign policy.

The text of the treaty states: "The High Representative (...) is responsible for the EU's common foreign and security policy"[92]. While the EEAS was created to execute a potential CFP, the CFP itself was not set out by the Treaty of Lisbon. However, it is the job of the High Representative both to apply and propose a CFP as well as convincing member states to follow through. The EEAS is autonomous in the organisation of the EU institutions, but its funding is provided by Parliament, which according to Mankhe is the most pro-european institution[93]. This means that Parliament would certainly support actions from the High Representative to increase areas of european integration of policy. Following this logic, Mankhe argues that the momentum has to come from Parliament which should give more power and budget to the High Representative in order to convince member states to follow a CFP and to promote the EU's geopolitical reach overseas.

The EEAS was a turning point in EU diplomatic history. After the Treaty of Lisbon, the EU's foreign policy shifted from mostly trade and development to actual diplomatic relations and political influencing. Diplomatic delegations became facilitators for the EU and the host nations not only in economic matters but also in political ones. These delegations already exist, and it would certainly be possible to create a diplomatic missions to Big Tech that would allow better techplomacy. These initiatives have to come from the High Representative, who is encouraged to do so by the Treaty of Lisbon, and be backed by the Parliament that should encourage greater european policy integration[94]. The article 21 of the Treaty of Lisbon also states that member states should mutually support each other, actively follow european external policies and avoid working against the interest of the Union. The tools are there. The EU simply needs to use them and convince member states to follow through.

[92]The Treaty of Lisbon. (2009, December 1). Retrieved from http://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon

[93] Mahncke, D. (2014). A post-modern foreign policy. *New Approaches to EU Foreign Policy*, 163-177. doi:10.4324/9781315771151-9

[94] Mahncke, D. (2014). A post-modern foreign policy. *New Approaches to EU Foreign Policy*, 163-177. doi:10.4324/9781315771151-9

The EU's unique regulatory position on the internet

Before any discussion of possibilities for diplomatic representation to tech companies, the EU must first define clearly what its role ideally should be concerning the internet. The recent increase in malicious cyber activities designed to destabilize Europe show that the need for greater EU influence on the internet is only growing, both for the sake of democratic stability in Europe and the safety of its citizens online. Patryk Pawlak, the executive officer for the European Union Institute for Security Studies argues that the strength of the EU when it comes to approaching internet regulation is the potential for wide ranging multidisciplinary efforts.

The growing importance of the internet, both as a potential digital battlefield and economic market, means that more and more state actors want to increase their control over it. Europol estimates that cybercrime robs the EU's economy of around €265 billions annually[95] and, as was argued at length earlier in this thesis, the social and democratic fabric of society is also at risk because of actions undertaken on the web.

Pawlak argues that core values of the EU for the internet such as openness, accessibility and safety are challenged by other major international players, mainly China and Russia. At the same time, while the EU still represents today a major fraction of internet traffic, the developing world will as soon as 2025 represent 75% of the global digital population[96]. The window of time for the EU to have a legitimate claim on shaping cyberspace is starting to close. Right now, internet governance is very fragmented and the EU's intergovernmental approach is not helping. Pawlak argues that right now, member states engage in nationalistic

[95] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.168.
[96] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.169.

policy making that results in suboptimal policies while the EU has the potential to do so much more[97].

Contrary to other international organisations which often focus on narrow missions (dealing with cybercrime, regulating commerce, protecting privacy), the EU has the unique opportunity to cast a much wider net in its approach to regulation of cyberspace. Its mandate is much larger than the other organisations currently trying to regulate some specific sector. The EU's unique position allows it to both take advantage of the opportunities and deal with the potential threats in a complex, multi-dimensional framework of regulation[98].

Pawlak describes this framework as a "partially overlapping and non-hierarchical institutions governing a particular issue area, without a single international agreement or authority but with a common focus"[99]. He defines this framework as the cyber regime complex, a dynamic playground that allows for the constant innovation of the internet and that introduces the need for actors to constantly cooperate in new ways to make sure that certain overarching values are followed but not a certain set-in-stone agenda designed by a hierarchy.

This cyber regime complex would allow for multiple understandings of a same event as different institutional actors might agree or disagree on the consequences of technological developments. If we understand technological development to be both risks and opportunities, only a complex regime can maximise its potential. As Pawlak puts it, the policy making process becomes a "struggle for ideas", which is what political discourse should be about. While the one-dimensional narrow international organisations can struggle to properly assess the long term-impact of certain technologies, such a complex regime wouldn't, Pawlak argues[100].

[97] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.172.
[98] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.179.
[99] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.170.
[100] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.176.

Due to this unique characteristic of the European Union, it is ideally placed to play a major role in shaping the internet through building a non-hierarchical complex cyber regime of competing, exchanging and cooperating institutional actors that create a fruitful dialogue around new technologies.

Chapter 3: Updating EU Diplomatic Representation in Silicon Valley

Existing Modes of Representation

The previous chapter defined the EU's unique position, opportunities, challenges and possibilities in the creation of a regulatory framework around the internet, as well as the need for cooperation with other state and non-state actors. Amongst these non-state actors, as was argued in the first chapter, the so called "Big Tech" companies are particularly important. This chapter will focus on the practical aspect of such cooperation and the ways in which the EU can create a fruitful environment that fosters the safe development of the internet.

In a recent publication from DiploFoundation, the authors argue that interaction between governments and tech companies happen on different level simultaneously. On an official level, intensive contact is made either politically or legally between the two as companies are often asked to appear in front of parliaments and courts or as they discuss investments and business deals. On an informal level, government officials and members of the tech industry often network to exchange information, build relationships and create trust. These interactions on an informal level serve to ease communication and interactions on an official level, so both of these are very complementary. Recently, academia has also been a place where governments and the internet industry meet, particularly on very technologically advanced subjects, none more so than AI. As these new technologies represent very important interests for both, the academical discussion shaping policy and innovation is becoming increasingly important. Finally, on an international level, summits are held

between government officials, international organisations and members of the tech industry. While the first of such major forums was the World Summit of the Information Society, today the most important one is the Internet Governance Forum[101].

Both parties participating in these interactions have to find a delicate balance. On the one hand, countries try to protect their citizens privacy while finding a competitive advantage for their businesses, and on the other hand, tech companies try to escape regulations but need the legitimacy and legal approval for their businesses to function. Because of this, both are open to a potentially mutually-beneficial dialogue. As seen earlier, one of the issues for the creation of a Common European Foreign Policy is that countries would have to give up their comparative advantage in order to potentially get bigger rewards in the long run. To achieve this comparative advantage, different countries have different methods that will be described below.

The first type of state representation is a consulate. More than seventy countries have a consulate around San Francisco which have often been in place before the internet and have been promoting economic or cultural interests of their host countries amongst Americans but also among their own citizens, as the area has been an attractive immigration destination since the gold rush[102]. Digital development in the area has then forced these consulates to adapt and expand their activities to this particular sector.

The main focus of these consulates is attracting investments to and from their countries in key technologies. These consulates can also create innovation centers that have branches in different tech sectors and promote networking with the internet industry, predominantly between its own expats. This is the case of Germany which uses this innovation center to bring technological development back to Europe as fast as possible, to conserve a comparative technological advantage with its neighbours through the knowledge of its own expats in the Bay Area[103]. Italy as well uses its consul as an unofficial tech ambassador, who

[101] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.4.
[102] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.16.
[103] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.17.

is tasked with establishing relationships with Big Tech companies and support small italian startups in the area. Mexico's consulate in this historically and geographically close region even has a specific agenda and mission. Mexico aims to attract investment in its own "Silicon Valley", around the city of Guadalajara, enticing tech entrepreneurs with lower costs of labour and living as well as a rapidly growing economy.

Countries such as China, India or South Korea also take advantage of their consulates to open access to the Bay Area tech sector for their own developed domestic tech sectors, facilitating exchanges. For these countries that boast an already well-developed tech sector, the aim is predominantly to encourage investment to and from Silicon Valley and try to stay on top and potentially even copy the technological innovation in the region[104].

Many European countries, however, bet predominantly on innovation centers which can be separate or attached from the consulate. These innovation centers are long term projects and investments that require a large presence in the area often based on strong expat communities. They can act, if attached to the consulate, as outposts designed to advance their countries' digital agenda by informing and organising events and conferences but they can also be accelerators and incubators for startups, either from the home country or to attract foreign startups to the home country.

Perhaps the most famous innovation center, still regarded as an example by many countries, is the swissnex model. This swiss funded innovation center is very independent, answers only to the Ministry for Education, Research and Innovation and chooses their own activities, focuses and projects. While a part of the funding comes from the State, swissnex is expected to find partners to help with financing and stimulates entrepreneurial exchange to and from the Bay Area. The idea behind swissnex is to allow this innovation center to think outside the box, adapt to trends quickly and innovate in the ways it can further swiss interests in the Bay Area, by making sure it "speaks the same language" as the local tech industry[105].

[104] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.18.
[105] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.20.

The Netherlands have a similar model and have been very successful in attracting investments and startups to its homeland and one of the world's most highly digitalised population. They do not act independently however, and report to the Consulate General of the Netherlands.

Other countries attach these innovations services with state investment agencies, such as the Czech Republic with CzechInvest, which are dedicated to assisting Czech businesses in the area with financial and networking support[106].

The First Tech Ambassador

Lately however, the newest model of diplomatic representation in the Bay Area that has been harnessing massive media attention has been Denmark's world first Tech Ambassador. Casper Klynge is a career diplomat whose new offices are based in Silicon Valley, Copenhagen and Beijing. His mandate is wide-reaching and mostly self-imposed from digital security, trade, cooperation to promoting danish interest and keeping the danish government up to date on technological innovation and its potential impact on Denmark. The role of the Tech Ambassador is two-fold as he can both inform policy and relevant ministries of the latest technological development and proactively guide technological development in a direction that matches Denmark's values and interests[107]. He does so by being a clear and constant relay between tech companies and the danish government who both benefit from his expertise, the first by being able to build products that will pass regulations and the second by being informed of the direction of technological development. This constant potential dialogue is the key to the Tech Ambassador position, particularly in a sector in which evolution moves so quickly and the consequences of such evolutions are often very important to civil society.

[106] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.21.
[107] Braugh, P. (2017, July 20). 'Techplomacy': Denmark's ambassador to Silicon Valley. Retrieved from https://www.politico.eu/article/denmark-silicon-valley-tech-ambassador-casper-klynge/

His office is staffed with career diplomats but also professionals from various backgrounds: tech sector, international organisations, media agencies, academia and even members from other Danish Ministries. The whole of government approach of this office leads the Tech Ambassador to work with all Danish Ministries and inform them from development in their particular field in order to better prepare Denmark for the future[108]. This initiative has been closely followed by other European countries such as France who has recently appointed an Ambassador for Cyberdiplomacy and the Digital Economy, with the aim of creating a direct dialogue with Big Tech.

In the announcement for the position of Tech Ambassador, the Danish Foreign Minister said the following: "We've been too naïve for too long about the tech revolution. We need to make sure that democratic governments set the boundaries for the tech industry — and not the other way around. That's where the Danish TechPlomacy initiative comes in"[109]. The justification for the role of the Tech Ambassador was laid out by Casper Klynge and his team in a recent edition of The Hague Journal of Diplomacy. He argues that the economy of Denmark, perhaps more so than other countries due to its small but advanced economy, has a lot at stake when it comes to technological innovation. However, he notes that "The Danish Foreign Ministry, like most other foreign services around the world, did not have a dedicated setup to effectively deal with the foreign policy dimensions of emerging technologies, including a way to engage the multinational tech giants in a structured manner."[110].

As this thesis has argued for, this gap described between the growing power of Big Tech and the inability of the diplomatic community to engage them is creating what Donaldson and Younane call the "diplomatic deficit". It is essential for the EU to drive societal change in a direction that is beneficial for its citizens and as it has itself been driven by technological innovation, the diplomatic system has to encompass these companies[111]. In justifying his role

[108] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.15.
[109] Satariano, A. (2019, September 3). The world's first ambassador to the tech industry. Retrieved from https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html
[110] Klynge, C., Ekman, M., & Waedegaard, N. J. (2020). Diplomacy in the digital age: Lessons from Denmark's TechPlomacy initiative. The Hague Journal of Diplomacy, p.187.(1-2), 185-195. doi:10.1163/1871191x-15101094
[111] Klynge, C., Ekman, M., & Waedegaard, N. J. (2020). Diplomacy in the digital age: Lessons from Denmark's TechPlomacy initiative. The Hague Journal of Diplomacy, p.189.(1-2), 185-195. doi:10.1163/1871191x-15101094

as a Tech Ambassador for Denmark, he argues: "For a government to rely solely on traditional diplomatic relations to bring home knowledge, promote its interest and safeguard values abroad, no longer seems sufficient."[112]. There is no reason why this statement can not be adapted to the EU.

Representing the EU

There is no official European Commission diplomatic representation as of now in the Bay Area, even though some institutions and organisations have offices there. In the second chapter, the reason why such an office would be difficult to create were laid out. The main problem lies in the ongoing competition between member states when it comes to attracting investment and gaining tech advantages. However, the potential impact of a united EU policy concerning the tech sector would be game-changing. As EU countries are responsible for more than half the foreign investment in tech companies, they certainly have the power to guide tech development in a direction that matches European values and bring the latest innovations to the EU as fast as possible[113].

The perspective of easy access to the common market should also be enough to attract investment and expertise back to the EU as companies might have a better chance of success if they already follow guidelines and regulations that would allow for this easy access. Tech companies are certainly interested in accessing the common market and in a recent interview Casper Klynge, the danish tech ambassador, jokingly said that half of his job was explaining the GDPR to US tech companies. This open constant dialogue policy attached to a clear person of contact is something the EU is missing. The famous line from Kissinger "Who do I call if I want to call Europe" seems to apply when it comes to the relationship between Big Tech and the EU.

---

[112] Klynge, C., Ekman, M., & Waedegaard, N. J. (2020). Diplomacy in the digital age: Lessons from Denmark's TechPlomacy initiative. The Hague Journal of Diplomacy, p.190.(1-2), 185-195. doi:10.1163/1871191x-15101094

[113] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.25.

The European Institute of Innovation and Technology is already an initiative in the right direction. This innovation center focused on digital innovation has become the informal basis for meetings and cooperation between representatives of member states[114]. During those meetings, member states representatives try to create a European network and, at times, pool resources for major projects. This is the closest thing to an official organisation that can be a designated point of contact that the EU has to offer.

The EU could draw inspiration from the Nordic Innovation House for its own representation in the Bay Area. Norway, Sweden, Finland and Denmark decided in 2014 to join their innovations centers together in a bid to encourage development of key technologies such as clean energy with an increased financial weight. Today, while all NIH partners have specific national mandates, they cooperate constantly on common projects directed by their long term goal of sustainable technological growth. This increased cooperation has allowed Nordic countries to undertake projects that were previously out of their financial reach and cooperate with larger companies that previously could have snubbed their smaller markets[115].

In conclusion, the EU can draw inspiration from several existing modes of diplomatic representation and the following steps can be taken to create a sustained mutually beneficial dialogue with tech companies.

First, the EU must convince its member states of the importance of an improved european diplomatic representation, which might be difficult due to the fact that, as of now, member-states compete with each other. Member-states who already have well-functioning innovation centers might be reluctant to let go of their comparative advantage for potential, non-guaranteed, long term benefits. To do so, it must show that international cooperation has been beneficial for other organisations in the past such as the NIH.

[114] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.21.
[115] Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). *The Rise of Techplomacy in the Bay Area*. DiploFoundation, p.23.

Second, it can also draw inspiration from the danish tech ambassador. While a unique ambassador is more adapted to a small country, several characteristics of this mode of representation can serve as inspiration for the EU. On the one hand, the idea that the Ttech ambassador's office interacts with all the different danish ministries bringing to the attention, for example, of the Ministry of Agriculture the latest development in that specific field. Such a proposition could be adapted to the European Commission, a whole-of-government approach that would see constant report from an European Tech Embassy to the concerned parts of the Commission to insure the EU is not missing out on the latest technological innovations. On the other hand, the EU could also imitate the international nature of the danish model, and with the greater financial backing, allow its own tech embassy to have offices all around the world, facilitating communication and creating a network that puts Europe in the middle of tech innovation. Finally, the EU should strive to create a constant communication channel to create a mutually beneficial dialogue that ensures that interested companies can develop future products in full knowledge of European regulations and that the EU can predict future technological change and prepare more adequately for these changes.

Third, the EU should build on what already exists rather than start completely new and risk lost opportunities. Member-states have been building networks and relationships with key actors of the tech sector for decades, and these relationships are very valuable. When nordic countries joined their innovation centers in the Nordic Innovation House project, they joined their existing networks together. The current national diplomats are well-versed in the unique environment that is Silicon Valley and have been forging valuable relationships. The EU needs to build on these existing networks and join them together by engaging with the large european expat community as a whole in the region and join the existing innovation centers rather than replace them. The EU must also create a broader network than simply tech companies and diplomatic representatives. Universities, think-tanks and other non-governmental organisations have an important role to play in debating policy-agendas and the impact of technological innovation. The EU must create a large and diverse network that allows it to create a constant discussion around technology and its impact.

On March 27 2019, the EU increased its support of the EIT initiative, which is certainly a step in the right direction. It seems however that even with increased backing, the EIT still does not have the resources to have more than two offices around the world (Israel and Silicon Valley) and its projects are still conducted in parallel with member-states rather than a true multinational initiative[116].

Conclusion

Regulating technological innovation requires a complex approach that takes into account the risks and rewards associated with it. Several tech companies, particularly the Big 5 (Apple, Amazon, Microsoft, Facebook, Google), now boast user bases larger than the biggest countries in earth and billion to trillion US$ budgets to accomplish their goals. These companies do not necessarily have citizens' best interests in mind, even though sometimes these may align with their business model. Companies such as Google have been instrumental in bringing technology, the internet and digital emancipation to many developing countries on Earth. Even though their motivation might have been more economical than humanitarian, they still result in boosting social change but these can also be interpreted as side-effects of their capitalistic goals.

This is not always a problem. For example, when Google brings connectivity to poor rural areas, they offer new opportunities and potential economic development while ensuring more and more people use their services and enter their business model. However, when Facebook orders their newsfeed in a way designed to maximise outrage in order to keep users on their site and watching ads, it becomes clearer that profit is the bottom line and not users' well being, no matter the humanistic claims made by its founder.

The impact these companies can have is only one side of the coin that explains why the EU should invest and upgrade its diplomatic representation in Silicon Valley. The potential

[116] European Institute of Innovation and Technology. (2020, January 21). Global outreach. Retrieved from https://eit.europa.eu/our-activities/global-outreach

benefits of new technologies can not be underestimated. As Klynge points out, the challenge and objectives of a diplomatic representation with Big Tech is double: "(to create) a direct and frank dialogue with the tech companies to try and influence the direction of technology and our own preparedness"[117].

This delicate and sometimes contradictory balance is illustrated in the recent comment of the European competition commissioner Margrethe Vestager. She offered a very optimistic view of the potential impact of AI on society: "there's no limit to how AI can support what we do as humans."[118] This same commissioner has built a reputation for being the harshest regulator of Big Tech after imposing a €4.3 billion fine on Google in 2018 and recuperating €13 billion illegal tax benefits from Apple in 2016. However, there is a logic behind this behaviour. Certainly, the potential impact of the technology developed by Big Tech can not be underestimated but, if left alone, there's no guarantee Big Tech will use these technologies for reasons in line with EUrope's vision for the future. As she added further: "But we need to get in control of certain cornerstones so that we can trust it, and it has human oversight"[119].

There is a delicate balance to strike between much needed regulation and innovation. Suffocating development is a mistake and any kind of regulation has to carefully design its policies to avoid certain issues. Indeed, the recent GDPR has been criticised for being comparatively more harmful to small companies as they might not have as much trust from their customers to accept their terms and conditions and the lack of sufficient financial backing to be able to adapt their product to fit the new regulations.

We can observe the EU starting to transition from cyber diplomacy to techplomacy in a shift that started with the Cambridge Analytica scandal in early 2018. Before the scandal, most of the EU's focus when it comes to cyberspace was centered around cyber warfare. Hacks, cyber attacks and other matters pertaining more to cyber security. It is only after the scandal

[117] Klynge, C., Ekman, M., & Waedegaard, N. J. (2020). Diplomacy in the digital age: Lessons from Denmark's TechPlomacy initiative. The Hague Journal of Diplomacy, p.192.(1-2), 185-195. doi:10.1163/1871191x-15101094

[118] EU competition commissioner Margrethe Vestager says there's 'no limit' to how AI can benefit humans. (2019, November 8). Retrieved from https://www.businessinsider.in/tech/news/eu-competition-commissioner-margrethe-vestager-says-theres-no-limit-to-how-ai-can-benefit-humans/articleshow/71963488.cms

[119] op. cit.

that the EU adapted their policies to focus on any and all sort of malicious digital activities, including propaganda, trolls, hack-and-leak operations and such. The damage these operations can do, while being in a grey area of legality, can be much more severe than cyber attacks. The web has become, as Powers and Jablonski put it, a battlefield of ideas where certain actors are ready to use any means necessary to further their interests[120]. It is time that the EU adapted their outlook on digital security to include things that don't traditionally fit in cybersecurity.

This is not to say that cybersecurity isn't important anymore, Missiroli argues that the number of cyber attacks has grown almost exponentially, but to protect and deter cyber attacks, Europe needs to build a resilient network built on multilateral agreements and cooperation between state and non-state actors[121]. Amongst these non-state actors, the most important ones are Big Tech companies, which explains the recent convocation Facebook's CEO Mark Zuckerberg in front of the European Parliament. Considering the interferences with the Brexit referendum and the US election were conducted in part on Facebook and had an important impact on the EU, it seems logical for the EU to try to work with them to avoid such interferences taking place again.

There are obstacles in the making of a common foreign policy for the EU. Even though the Treaty of Lisbon confers to the High Representative the power to define it, the biggest obstacle is the member states, Dieter Mahncke argues. The biggest member-states are reluctant to pool all their resources together in the region because of the important effort they have put into building networks in the Bay Area and the comparative advantage this procures their national economies against their neighbours. Even though a common foreign policy would certainly have beneficial long term consequences, on the short term the pill is hard to swallow.

Patryk Pawlak argues however that the potential for the EU in regulating cyberspace is unique. While most other organisations focus on one aspect (fighting cybercrime, regulating

[120] Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press,. p.198.
[121]Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. *European Foreign Affairs Review*, *2019*(2), p.141.

cryptocurrencies, etc.), the EU's mandate is much larger. The EU can approach issues from different directions as its goal is simply to better the life of its citizens. Pawlak argues that the EU should create a complex cyber regime of different organisations public and private that debate, cooperate and argue over the impact of certain new technologies in what he calls a "struggle for ideas" that is "the very stuff of democracy"[122].

This network of organisations could be based on the current member-states infrastructure there and the network they worked very hard to build. Each country has a more or less unique method of representation that focuses on slightly different diplomatic aspects or investments. The EU should draw lessons from innovations in diplomatic representation from certain member states, perhaps none more so than Denmark and its world-first tech ambassador. Such an office would be ideal to create the constant dialogue necessitated to better interact with Big Tech companies. Europe should also certainly observe the Nordic Innovation House and their model cooperation and pooling of resources on certain projects to make sure that the EU has both as big of an impact as possible on the direction of technological innovation and the opportunity to invest and stay up to date the latest impactful technological developments that could help or hurt Europe in the future.

Bibliography

About the Global Tech Panel. (2019, January 11). Retrieved from https://eeas.europa.eu/headquarters/headquarters-homepage/50886/about-global-tech-panel_en

Albrecht, J. (2016). How the GDPR Will Change the World. European Data Protection Law Review, 2(3), 287-289. doi:10.21552/edpl/2016/3/4

Apple Market Cap | AAPL. (2019, October 14). Retrieved October 14, 2019, from https://ycharts.com/companies/AAPL/market_cap

[122] Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, *24*(2), p.170.

Assange, J. (n.d.). Google Is Not What It Seems. Retrieved from https://wikileaks.org/google-is-not-what-it-seems/

Babel, C. (2020, May 7). The high costs of GDPR compliance. Retrieved from https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263?

Bay Area Council Economic Institute Report. (2014). Europe and The Bay Area: Investing in Each Other.

Benson-Rea, M., & Shore, C. (2011). Representing Europe: The Emerging 'Culture' Of EU Diplomacy. Public Administration, 90(2), 480-496. doi:10.1111/j.1467-9299.2011.01997.x

Bjola, C., & Holmes, M. (2015). Digital Diplomacy: Theory and Practice. London, England: Routledge.

Braugh, P. (2017, July 20). 'Techplomacy': Denmark's ambassador to Silicon Valley. Retrieved from https://www.politico.eu/article/denmark-silicon-valley-tech-ambassador-casper-klynge/

Cerulus, L. (2018, May 23). Mark Zuckerberg dodges punches at European Parliament. Retrieved from https://www.politico.eu/article/mark-zuckerberg-dodges-punches-at-european-parliament/

Dance, G., LaForgia, M., & Confessore, N. (2018, December 18). As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. The New York Times.

Doffman, Z. (2019, September 9). Russia Accuses Facebook And Google Of Illegal Election Interference. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/09/09/russia-slams-facebook-and-google-with-new-allegations-of-election-interference/#1655f30b5940

Donaldson, A., & Younane, I. (2018, February). A diplomatic deficit? The rise of non-state actors. Retrieved from https://www.britishcouncil.org/research-policy-insight/insight-articles/diplomatic-deficit-actors

The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data. The Economist.

EU competition commissioner Margrethe Vestager says there's 'no limit' to how AI can benefit humans. (2019, November 8). Retrieved from https://www.businessinsider.in/tech/news/eu-competition-commissioner-margrethe-vestager-says-theres-no-limit-to-how-ai-can-benefit-humans/articleshow/71963488.cms

European External Action Service. (2016). Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy.

European External Action Service. (2017). The EU Global Strategy – Year 1.

European External Action Service. (2018). The EU Global Strategy – Year 2.

European External Action Service. (2019). A New Strategy Agenda: 2019-2024.

European External Action Service. (2019). From Vision to Action: The EU Global Strategy in Practice - Three years on, looking forward.

European Institute of Innovation and Technology. (2020, January 21). Global outreach. Retrieved from https://eit.europa.eu/our-activities/global-outreach

Facebook isn't free speech, it's algorithmic amplification optimized for outrage – TechCrunch. (2019, October 20). Retrieved from https://techcrunch.com/2019/10/20/facebook-isnt-free-speech-its-algorithmic-amplification-optimized-for-outrage/

Google Unveils Tools to Access Web From Repressive Countries. (2013, October 21). Retrieved from http://business.time.com/2013/10/21/google-digital-rebels/

Google's Diplomatic Edge. (2019, March 28). Retrieved from https://www.googletransparencyproject.org/articles/googles-diplomatic-edge

Gorwa, R. (2019). What is Platform Governance? Information, Communication & Society, 22(2019), 854-871.

Gorwa, R., & Peez, A. (2019, June 27). Big tech hits the diplomatic circuit. Retrieved from https://berlinpolicyjournal.com/big-tech-hits-the-diplomatic-circuit/

Hill, A. (2018, November 2). The global hunt to tax big tech. Retrieved from https://www.ft.com/content/79b56392-dde5-11e8-8f50-cbae5495d92b

Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). The Rise of Techplomacy in the Bay Area. DiploFoundation.

Horejsova, T., Ittelson, P., & Kurbalija, J. (2018). The Rise of TechPlomacy in the Bay Area. Retrieved from https://issuu.com/diplo/docs/techplomacy_bayarea

Khamis, S. (2015). Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies (Doctoral dissertation, University of Maryland).

Kirkpatrick, D. (2011). Does Facebook have a foreign policy ? Foreign Affairs, 190. Retrieved from https://www.jstor.org/stable/pdf/41353271.pdf?refreqid=excelsior%3Ad5fed7e7771dbae069f2babfb6574d03

Klynge, C., Ekman, M., & Waedegaard, N. J. (2020). Diplomacy in the digital age: Lessons from Denmark's TechPlomacy initiative. The Hague Journal of Diplomacy, 15(1-2), 185-195. doi:10.1163/1871191x-15101094

Mahncke, D. (2014). A post-modern foreign policy. New Approaches to EU Foreign Policy, 163-177. doi:10.4324/9781315771151-9

Marzouki, M. (2019). "Techplomacy": Towards an Increasingly Privately Ordered Digital World Politics? Toronto, Canada: International Studies Association.

Mateusz, M. (2018, May 2). Techplomacy: Denmark's bridgeway to Silicon Valley. Retrieved from https://www.diplomacy.edu/blog/techplomacy-denmarks-bridgeway-silicon-valley

Matsakis, L. (2019, February 15). The WIRED Guide to Your Personal Data (and Who Is Using It). WIRED.

Microsoft Market Cap | MSFT. (2019, October 14). Retrieved October 14, 2019, from https://ycharts.com/companies/MSFT/market_cap

Missiroli, A. (2019). The Dark Side of the Web: Cyber as a Threat. European Foreign Affairs Review, 2019(2), 135-152.

Paris call for trust and security in cyberspace — Paris call. (2018, November 13). Retrieved from https://pariscall.international/en/

Pawlak, P. (2019). The Eu's Role in Shaping the Cyber Regime Complex. European Foreign Affairs Review, 24(2), 167-186.

Powers, S. M., & Jablonski, M. (2015). The Real Cyber War: The Political Economy of Internet Freedom. University of Illinois Press.

Reuters. (2019, September 6). Russia Says Facebook, Google Must Ban Political Ads During Moscow Election. Retrieved from https://www.themoscowtimes.com/2019/09/06/russia-says-facebook-google-must-ban-political-ads-during-moscow-election-a67189

Satariano, A. (2019, September 3). The world's first ambassador to the tech industry. Retrieved from https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html

Scola, N. (2014, December 18). At the heart of Obama's Cuba doctrine? The Internet. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/at-the-heart-of-obamas-cuba-doctrine-the-internet/

Shaban, H. (2018, January 23). Google for the first time outspent every other company to influence Washington in 2017. Retrieved from

https://www.washingtonpost.com/news/the-switch/wp/2018/01/23/google-outspent-every-other-company-on-federal-lobbying-in-2017/

TechPlomacy: Reinventing Diplomacy in the Digital Era (Casper Klynge, Tech Ambassador of Denmark) [Video file]. (2018, May 21). Retrieved from https://www.youtube.com/watch?v=pWABDF3J6YU

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. Journal of Democracy, 28(4), 46-59. doi:10.1353/jod.2017.0064

Waterson, J. (2018, May 23). Five things we learned from Mark Zuckerberg's European Parliament appearance. Retrieved from https://www.theguardian.com/technology/2018/may/22/five-things-we-learned-from-mark-zuckerbergs-european-parliament-appearance

West, S. M. (2014). Redefining Digital Diplomacy: Modelling Business Diplomacy by Internet Companies in China. The Hague Journal of Diplomacy, 9(4), 334-355. doi:10.1163/1871191x-12341295

World GDP Ranking 2019. (2018, April 2). Retrieved October 14, 2019, from http://statisticstimes.com/economy/projected-world-gdp-ranking.php

Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. Seton Hall Law Review, 47(4), 995-1020.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.