EIIS | EUROPEAN INSTITUTE OF INTERNATIONAL STUDIES

GLOBAL POLICY PERSPECTIVE REPORT

Techplomacy and the Tech Ambassador

Shaun Riordan & Mario Torres Jarrín

This work is published by the European Institute of International Studies.
Printed in Salamanca-Stockholm, January 20, 2020.

Contents

Techplomacy and the Tech Ambassador

Executive Summary

- The Danish appointment of a Tech Ambassador was astute and far sighted. But the world has moved on, and the role of the Tech Ambassador, and Techplomacy, has expanded.

- Technology and internet companies play a crucial role in shaping the international environment. Governments and their diplomats need to engage with them at an international level, to understand better how they function and what new technological developments are in the pipeline, and their political and geopolitical implications. This is particularly true of countries and regions that are relatively weak in the technology sector (like the UE).

- Tech Ambassadors also have a crucial role in engaging technology and internet companies in the crucial debates about internet governance, whether the future of ICANN, the protection of data or net neutrality. But this engagement should extend also to international crime, both the ways in which new technologies can facilitate crime, and the ways in which internet and technology companies can better collaborate in its control.

- Internet and technology companies increasingly function like geopolitical actors in their own right, whether facilitating disinformation or fake news campaigns, issuing their own international currencies or through the new debates about international industrial standards. Claims to just be neutral platforms for the exchange of information are no longer credible.

- Tech Ambassadors should treat internet and technology companies as geopolitical actors, explaining their responsibilities and making clear the price of non-collaboration.

- Techplomacy must develop a more strategic approach to the tech sector as new companies from a broad range of countries and regions emerge. Technology will be ever more tightly tied to geopolitical competition. Tech Ambassadors will no longer be dealing with individual technology or internet companies, but rather consortia tying together related and complementary technologies.

- In as far as they are seen as geopolitical actors, technology and internet companies need to develop their own Techplomacy, whether for managing competing pressures in a geopolitically volatile world, presenting geopolitically

controversial products (like digital currencies) or navigating the mine fields of international competition for technological hegemony.

Introduction

Diplomacy engages with technology along three vectors: agency, process and content. A separate policy briefing, on Cyberdiplomacy, has examined the application of diplomacy to the political and geopolitical problems arising in cyberspace (subject matter). This policy explores the relationship between diplomacy and technology through agency, and specifically through the idea of appointing ambassadors to the technology sector.

In 2017 Denmark appointed an Ambassador to the high technology sector, commonly known as Denmark´s Tech Ambassador. France and Germany followed suit in 2018. However, the French Ambassador appears to be mainly concerned with preventing the use of social media and search machines to promote terrorism. Following a meeting with the German Envoy for Technology and Digitalisation, Denmark´s Tech Ambassador Caspar Klynge tweeted that there was significant overlap between their roles, but it is not clear what this is. The German Envoy is not an ambassador to the technology sector as such, and his role seems more ambiguous and less innovative. Neither the French nor German diplomats have secured the profile of their hyperactive Danish colleague.

The Danish Tech Ambassador is not the first time a country has opened a diplomatic mission related to cyberspace. The Swedes famously opened an embassy in the virtual world “Second Life”, although Second Life proved short lived and the Swedish Embassy had the feel of a gimmick. Several countries, especially those with limited resources, have opened virtual embassies, which offer information and services online in foreign countries. But these are cases of diplomacy taking advantage of digital tools, either to improve reach or to save resources, (often called “Digital Diplomacy”) rather than engaging with the generators of new technologies as diplomatic actors. In this sense the Danish move is a first and innovative.

The Role of the Tech Ambassador

The Office of Denmark´s Tech Ambassador (as Klynge´s embassy is officially called), is not limited to one physical site (as would be the case with a bilateral embassy), but split across three sites: Silicon Valley, Copenhagen and Beijing. There is talk of opening a further office in East Africa. Klynge has coined the term Techplomacy to refer to his role (and has launched a podcast “Techplomacy” to explore and promote it further). Klynge has described the key roles of his mission as:

- Gathering information on new and future technological developments and analysing their impact on diplomacy, politics and Danish society;

- Gathering information on developments within the technological sector itself, relations between tech companies and their plans for future operations/investments;
- Discussing ethical and regulatory issues with technological companies, with a focus on unacceptable content and data and privacy protection;
- Convincing technology companies to base operations, research facilities or European subsidiaries in Denmark;
- Promoting Denmark as a highly digitalised country at the cutting edge of new technologies and thinking (Klynge´s appointment as Denmark´s Tech Ambassador itself contributes to this).

Klynge´s description of his role raises several interesting issues:

- The different offices out of which he operates (Silicon Valley, Copenhagen and Beijing) give a fair idea of where Denmark sees as centres of technological innovation in the 21st century, as do the plans for a further centre in East Africa. It is interesting that they have not situated an office in the EU (other than the office in Copenhagen, which effectively gives Klynge a home base). But then it is also interesting that it is the Danish Foreign Ministry, rather than the European External Action Service, that has taken the initiative to set up a Mission to the Tech Sector.

- Although Klynge proclaims a new kind of diplomacy, Techplomacy for his mission, his job description looks remarkably like that of a traditional Ambassador or Embassy: gathering and analysing information about the country in which he is stationed and its implications for his home country; engaging the host government in discussions about regulatory issues and international law (particularly relevant in EU countries); engaging with the commercial and financial sectors to attract Foreign Direct Investment (FDI); and the promotion of his own country. The only two key activities of traditional embassies missing are engaging with the host government on geopolitical issues (but see below) and consular protection. The latter may be implicit, however, in the discussion of ethical and regulatory issues – at least in part aimed at the protection of the rights of Danish citizens in cyberspace. It is not that the diplomacy is different, but that its target has changed, reflecting the development of cyberspace and the importance of technology companies.

- Indeed, Klynge´s appointment recognises the importance of technological developments, especially in digitalisation, artificial intelligence and machine learning, to the development of international relations, and to the physical and economic security of countries like Denmark.

- On the Mission to the Tech Sector´s webpage, Klynge explicitly recognises that "Techplomacy" should be seen as complementary to traditional diplomacy. Klynge is seeking to build multi-stakeholder platforms with the tech sector, and other groups or individuals interested in the key issues, which can support the

effort of his colleagues working with governments and international organisations.

- The Mission also implicitly recognises internet and technological companies as geopolitical players in their own right, who are shaping the geopolitical environment in both physical and cyberspace, and in which states have to operate. This is not the first time that private companies have shaped the geopolitical environment – it could be argued that both telecommunication and oil companies have done so in the past. But no country in the past has felt the need to create a Mission and Ambassador specifically to these sectors. Something has changed.

Much of the work Klynge appear to be doing so far (to judge from the Mission webpage and his Twitter feed) has focused on Public Diplomacy-like activities to engage with Internet and Technology companies, but also with a wider public to promote understanding of his mission. Thus he has been participating in a series of conferences and workshops, including attendance at the UN General Assembly. But he has also launched "Ambassador for one Day", in which US university students (interestingly not Danish university students) can compete to spend one day replacing Klynge as Denmark´s Tech Ambassador. These Public Diplomacy activities no doubt help establish the standing and credibility of Denmark´s Mission to the Tech Sector, and as such contribute to the Mission objectives/job description (as set out above). However, there are other issues about how Klynge and his team relate to the Tech Sector, and in particular Internet Companies (especially social media platforms and search engines).

Internet Governance

There is the question of the debates about internet governance. These debates cover both the technical (but still highly politicised) issues of how to manage the internet (eg the role and status of ICANN, net neutrality, data protection, encryption or hate/racist content) and the efforts to establish basic norms of behaviour that may be able to constrain the various forms of cyber conflict. As with the implications of digital technologies for diplomacy and international relations, governments and diplomats have been slow to apply diplomacy to the problems arising in cyberspace, and understand that they cannot rely just on technical solutions. But gradually a serious of fora have emerged where these issues can be discussed, albeit with limited success or agreement.

In as far as he is engaging with internet companies about regulatory and ethical issues, Denmark´s Tech Ambassador, de facto at least, is already discussing internet governance issues with them. His advocacy of multi-stakeholder diplomacy to deal with the issues reflects the multi-stakeholder approach adopted by western governments to internet governance (although the commitment of the current US administration to this approach, especially after the decision to drop net neutrality, must be questioned). The multi-stakeholder approach essentially argues that internet governance should be debated and implemented through the broad range of state and non-state actors with interests in the internet, including companies, NGOs, technicians and users. This

approach is opposed by the "cyber sovereignty advocates" who argue that the internet is a public good and its governance should be purely inter-governmental. Klynge´s reference to "Techplomacy" complementing more traditional forms of diplomacy suggests that he will work with his colleagues in Denmark´s bilateral embassies when engaging with other governments. At the same time, his multi-stakeholder approach to relations with the Tech Sector, and his current Public Diplomacy activities, leave him well-placed to engage with a broad range of non-state actors, including internet companies but also users groups, technicians and others. The key question is to what extent he will seek to influence thinking within the Tech Companies, especially the Internet Companies, to encourage them to make common cause with Denmark and others against the Cyber Sovereignty Advocates. In other words, to what extent will he move beyond building networks of information and influence to actively constructing coalitions to advance Denmark´s policy positions. A second question, is to what extent internet companies, especially social media platforms and search engines, will be willing to tie their flags to the mast, even if they agree with the outcomes Denmark is seeking, if it might put their commercial interests at risk, especially if they are operating or seeking to operate in the territories of cyber sovereignty advocates.

Organised Crime

The new technologies developed or rolled-out by internet and technology companies have opened up significant opportunities for organised crime, in particular child sexual abuse (both transmitting images and grooming), money laundering and human trafficking. Internet and technology companies often get caught between their desire to protect the privacy of their clients and the need to combat these crimes. Collaboration with the authorities in closing down web-pages or denying individual users access to their services is often half hearted. The encryption debate, and the danger that expanding end to end encryption (for example across all Facebook platforms) poses to children and other victims of online crime, has not been fully taken on board. Together with data protection and internet governance, engaging internet and technology crime on issues relating to organised crime, and persuading them to engage with international protocols and agreements on fighting online crime (eg the Budapest Convention) as a key priority will also form part of the Tech Ambassador´s role.

Internet Companies as Geopolitical Actors

Secondly there is the question of to what extent a Tech Ambassador can, or should, engage with Internet Companies, especially social media platforms and search engines, as geopolitical actors in cyberspace conflict. The companies themselves are reluctant to see themselves in these terms. Facebook is still coming to terms with the growing public perception that, rather than a positive platform for promoting social networking, it is a mechanism for monetising data. However, countries like Russia are actively using platforms like Facebook and YouTube as part of their information warfare campaigns to destabilise western societies. While Facebook, Youtube and Twitter claim that they block doubtful accounts, this misses the point. The problems lie deep in the architecture

of social media platforms. The algorithms which ensure that users get only the advertisements and friend proposals likely to appeal to them, also limit the news and opinions they receive to those likely to appeal to their existing biases and prejudices. Social media platforms did not invent echo chambers, but the way they function reinforces them, further polarising social and political debate. "Information warriors" are able to take advantage of the same algorithms to ensure that the fake news stories they create reach the echo chambers already predisposed to believe them. In the case of Facebook, they are also able to take advantage of the groups which Facebook promotes to enhance social networking on the platform to draw vulnerable users into networks of fake news and conspiracy theories. Although most of the media focus on social media misbehaviour has fallen on Facebook and, to a lesser extent, Twitter, the real danger to Western societies may in fact prove to be YouTube. As levels of reading, and real literacy, fall in western societies, increasing numbers of people rely on videos for their news and opinions. Information Warriors increasingly make use of the algorithms underlying YouTube (which function in similar ways, and for similar reasons, to those which underlie Facebook) to ensure that their inflammatory and fake news documentaries reach the right audiences.

Search engines also offer opportunities for information warfare. The algorithms underlying search engines like Google order the pages in response to any given search. The aim of anybody seeking to influence Google users is to get their webpage or blog onto the first page of a search response (on the principle that few users go beyond the first page of responses). This can be done by paying Google, in which case it will indicate that it is an advertisement, reducing the credibility. The alternative is to take advantage of the underlying algorithms by using what are called "search engine optimisation" techniques. These construct webpages or blogs in such a way that Google is more likely to pick them up and locate them on the first page of responses. Such techniques are widely used by digital marketers and journalists. But they can also be used for nefarious purposes. In 2016 a group of neo-Nazis gamed Google´s algorithm so that of the first ten responses to the question "How many people died in the Holocaust?", seven were pages by holocaust-denier groups. The scope for using search machine algorithms to prioritise fake news responses to search enquiries is clear.

Social media platforms and search engines respond to these problems by claiming that they are neutral platforms, innocent victims of information warfare manipulation. But it is not altogether convincing. While their architecture facilitates information warfare, it frustrates public diplomacy. Because public diplomacy, unlike information warfare, is avowed, its messages must be coherent. It cannot segment its messages as information warfare can (targeted different messages on different echo chambers). As a result, the same algorithms, which ensure that information warfare´s fake news gets to the echo chambers predisposed to believe it, ensure that public diplomacy messages only reach those who already agree with it. It limits the ability of public diplomacy to engage with those who do not agree with it.

There is, however, a more serious point about the neutrality of social media platforms and search engines. In international law, the claim of neutrality by a state entails both privileges and obligations. One of the obligations is that a neutral state cannot allow the forces of a second country to cross its territory to attack a third country. If it does so, it becomes a belligerent in effective alliance with the second country. If it seeks to prevent

the passage of its territory by the second country, it also becomes a belligerent, in effect in alliance with the third country. This was the dilemma faced by Belgium in August 1914. By resisting the German passage across its territory to attack France, Belgium became an ally of France and the UK against Germany. There is a parallel with the situation of social media platforms and search engines confronted by Russian information warfare. If social media platforms like Facebook and YouTube continue to allow Russian and other countries´ information warfare to use the deep architecture of their platforms to destabilise western societies, then they in effect become allies of those countries. Taking down the occasional nefarious page or blocking the occasional questionable account does not meet the point if the information warfare is still able to take advantage of the deep architecture. On the other hand, if the social media platforms and search engines do collaborate more fully with western governments (which would include sharing information about how their algorithms work) they would in effect become allies of those western governments in combatting information warfare. This is the cyber equivalent of the dilemma faced by Belgium in 1914, and like Belgium, social media platforms and search machines that do collaborate with western governments could open themselves up to retaliation.

Cryptocurrencies

Recent events have reinforced the perception of Internet and technology companies as geopolitical actors in their own right, whatever they themselves may claim. Facebook´s plans to issue its own cryptocurrency Libra (in fact a digital currency backed by a basket of currencies and equities, rather than a true cryptocurrency) has clear geopolitical implications, which Facebook itself seems to have underestimated. Apart from the dangers of money laundering and other illegal activities taking advantage of a currency unregulated by any central bank, a global digital currency of the kind to which Facebook appears to aspire threatens to undermine the international reserve currency status of the US dollar. This reserve currency status of the dollar affords the US significant geopolitical advantages. Firstly, it enables the US to run fiscal deficits that would be unsustainable for other countries. But possibly more significant, it also allows the US to impose unilateral sanctions on countries, backed up by secondary sanctions on companies which then breach those sanctions. It is able to do so because the dollar remains the international currency of trade, and companies need to be able to trade in dollars, making them vulnerable to secondary sanctions. The most recent example has been the US´ unilateral imposition of sanctions on Iran following President Trump´s withdrawal from the Iran nuclear deal (JCPOA). Despite the other signatories to the JCPOA not following suit, and the EU specifically denouncing the US sanctions and encouraging European companies to continue trading with Iran, European as well as US companies have suspended trade with Iran for fear of US secondary sanctions.

There have been various proposals for bypassing the power of the US dollar. Other currencies, including the euro, rouble or renminbi, have been suggested as alternative international trading currencies. But none has yet secured sufficient credibility to do so, and the need to convert them at some stage into dollars fails to solve the vulnerability to secondary sanctions. Cryptocurrencies, whether bitcoin or nationally created digital currencies have also been suggested. But technical issues meant that they could not

handle the number of transactions to substitute in international trade for the dollar. With Libra, Facebook appears to have resolved the technical problems. Its millions of global users give it a scale and credibility which could pose a threat to the dollar´s reserve status over time. At the very least, the announcement of Libra encouraged China to advance the development of its own digital currency. Facebook´s insistence on seeing itself as a commercial rather than geopolitical actor caused it considerable problems with the launch of Libra. Rather than taking account of the regulatory and geopolitical issues that Libra would provoke, and developing a diplomatic strategy for mitigating them based around building coalitions of sympathetic state and non-state actors, Facebook launched it as just another commercial product. The inevitable back lash from central banks, other regulatory bodies and the US Congress has called the future of Libra into question. This suggests that it is not only a question of governments developing a techplomacy to deal with the tech sector. Technology companies, in as far as they are functioning as, or are perceived to be functioning as, geopolitical actors need to develop their own diplomatic capabilities.

International Industrial Standards

This impression is strengthened by the problems surrounding the roll-out of 5G mobile telephony, and in particular the role of the Chinese company Huawei. Although the media controversy has centred around security concerns, and the company´s relationship with the Chinese government and security services, a more interesting longer term issue may be the setting of international industry standards. Traditionally international industry standards for new technologies have been set by US companies or companies based in US allies. The second phase of 5G, relevant to the interconnection of devices in the internet of things (IoT), is the first time that significant industry standards for a new technology have been set by a company based in a US rival, namely Huawei in China. This threatens US hegemony in technological standards setting, and suggests that international industry standards meetings, previously rather dull events for techies, will become new battlefields for geopolitical influence. This both suggests a new area of activity for Techplomacy, and a new item on the agenda of the Tech Ambassador, and the need for technology companies to develop their own diplomatic capabilities to defend their interests in these conflicts.

The Huawei case should also alert us to the growing importance of non-Western technology companies. The Danish government has already recognised this by basing its Tech Ambassador partly in Beijing. Whereas the European Commission has previously focused its attention on the big US technology countries, and largely drafted its technology related directives to regulate their activities, the new challenge will be engaging with Chinese companies. Chinese technology companies are increasingly entering EU countries. The Spanish department store chain El Corte Ingles has announced that it will accept Chinese digital payment systems like Alipay (to facilitate Chinese tourism). Unlike US technology companies, Chinese companies tend to work together, offering technology packages, for example linking smart city technologies to 5G to ultra high voltage electricity transmission. Thus managing the interaction with Chinese technology companies will not simple be a question protecting data or ensuring the payment of taxes in the country where services are offered (which have been the

main issues with US companies). A more strategic approach to techplomacy will be needed. New technologies, and new techplomacy challenges, will arise not just in China, but also in countries like India and, if the Danish government is correct, in East Africa.

Conclusion

The Danish government appointed a Tech Ambassador to develop Denmark´s relationship with the Tech sector, promote Denmark as a centre for technology innovation and ensure that Denmark remains abreast of the latest technological developments. His role is also to engage in debates about technology regulation and issues such as data protection. But the world has moved on significantly since his appointment. The use of social media platforms in disinformation operations, the attempt by a social media platform to launch its own global currency and the debates about the involvement of technology companies with their governments and the setting of international industrial standards have all reinforced the idea of technology companies as geopolitical actors in their own right, with the privileges and responsibilities that such actors enjoy. This suggests that the remit of the Tech Ambassador may have to expand to treat the tech sector as one would nation states, and not always as friendly ones. If technology companies refuse to cooperate fully in combating government driven disinformation campaigns and fake news, they become complicit in those campaigns. If they fail to cooperate fully in combating crimes like human trafficking or child abuse, they become complicit in those crimes. And they risk being treated accordingly. But at the same time the Tech Ambassador should be actively seeking to recruit them into coalitions to shape the debates about internet governance and regulation, as partners in the construction of international norms and rules of the game in cyberspace.

Similar questions arise about the technology and internet companies themselves. If they are geopolitical actors, or are perceived as such, they need to develop their own techplomacy capacities. As shown by Facebook´s clumsy launch of Libra, if you aspire to a role that others perceive as geopolitical, you need to develop a diplomatic approach or strategy, regardless of your self-perception as a commercial company. Likewise, technology companies navigating through the newly dangerous minefields of international industry standards meetings will need diplomacy as well as technical skills, not just to secure the right to set industrial standards in the first place, but also to survive the geopolitical disputes of the subsequent technology roll-outs.

Denmark´s appointment of a Tech Ambassador was astute and far-sighted. It was not the publicity stunt some described it as at the time. It is surprising that other countries, or organisations like the EU, have not followed suit. But events have moved on, and the role and importance of the Tech Ambassador and Techplomacy have increased. Internet and technology companies are no longer exclusively western. Their geopolitical role is well-established. They can either become allies in dealing with the geopolitical and political challenges that new technologies pose, or they can become rivals to be dealt with accordingly. The techplomacy of both sides will decide which.

About the authors

Shaun Riordan is Director of the Chair of Diplomacy and Cyberspace of the European Institute of International Studied, a Senior Visiting Fellow of the Netherlands Institute for International Relations and senior diplomatic trainer with UNITAR. He has taught in diplomatic academies in Spain, Armenia, Bulgaria, Mongolia, Qatar and the Dominican Republic. Shaun is a former British Diplomat who served in the UN, Taiwan, China and Spain, as well as the UN, Far Eastern, Counter-Terrorism and East Adriatic Departments of the Foreign and Conmonwealth Office in London. He is the author of "The New Diplomacy" (2003), "Adiós a la Diplomacia" (2005), "Cyberdiplomacy; Managing Security and Governance Online" (2019) and "The Geopolitics of Cyberspace: a Diplomatic Perspective" (2019).

Mario Torres Jarrín is Director of the European Institute of International Studies (Sweden) and Director of International Relations at Pontifical University of Salamanca (Spain). He is Executive Secretary IBERO-EURO-AMERICA Consortium of Universities, Institutes and Institutions; Academic Council Member at Latin America and Caribbean-European Union Academic Forum; Member of the Task Force G20/20 Summits "The future of work and education for the digital age"; Research Group Member in Jean Monnet Project "Relations between the European Union and Latin America: Future scenarios in a changing world", and Research Group Member in Jean Monnet Project "Over the Atlantic. EU and Latin American Relations: Between Diplomacy and Paradiplomacy". He holds a PhD in History, a Master in European Union Studies, and a BA in Business Studies from the University of Salamanca (Spain).