EIIS EUROPEAN INSTITUTE OF INTERNATIONAL STUDIES

Global Policy Perspective Report Cyberdiplomacy

Shaun Riordan & Mario Torres Jarrín

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

Contents

Ciberdiplomacy

"La guerre! C´est une chose trop grave pour la confier à des militares". Clemenceau

Executive Summary

- Cyberspace is too important to leave to technicians (or intelligence officers). Diplomats too must engage in the key issues, including internet governance and cybersecurity.
- Cyberspace can be conceived as 4 layers: physical, logic, data and social. All four are political and geopolitical.
- The key issues in internet governance (ICANN, net neutrality, encryption, data protection, unacceptable content) are not technical. They require diplomats engaging at an international level.
- In cybersecurity technical measures are necessary, but not sufficient. Key issues centre on who wants to do what and why. At an international level diplomats are needed to analyse motivations and intentions, and to mitigate the risks of escalation and conflict.
- The application of international law to cyberspace is not straightforward, or universally accepted. Norms of behaviour in cyberspace will need to be constructed from the bottom up. Diplomats will need to use networks of contacts with state and non-state actors to identify shared preferred outcomes which can serve as the building blocks of an international law in cyberspace.
- Internet governance in particular will require diplomats to develop the capacity for multi-stakeholder diplomacy, building relationships with a broad range of state and non-state actors at the same time.
- The role of diplomats in cybersecurity is similar to their role in physical space. Managing inter-state relationships in cyberspace will require diplomats to socialise state (as well as non-state) actors into an international cybercommunity, with clear costs of not being a member of that community.
- Foreign Ministries must bring internet governance and international cybersecurity to the centre of their foreign policy and international strategies. They must ensure that their diplomats have the knowledge and skills to play effectively their role in managing international governance and security online.

Introduction

Cyberdiplomacy is the application of diplomacy to the problems generated in cyberspace. Until recently there has been the perception that because the internet was created by technicians, its problems are essentially technical and have technical solutions. This is reflected in the Internet Corporation for Assigned Names and Numbers (ICANN), the not-for-profit private sector corporation registered under Californian state law responsible for much internet governance. ICANN´s board of directors consists of technicians, specialist lawyers and industry representatives. Government representatives, again mostly technicians, are consigned to an advisory committee. And yet the key problems of internet governance (including ICANN´s status) and cybersecurity are political and geopolitical, touching on issues of sovereignty, social and foreign policy, international law and balance of power. Cyberspace is developing its own geopolitics, which shape the behaviour of both state and non-state actors. The political and geopolitical issues in cyberspace are inter-connected, and meld with parallel problems in physical space. Leaving cyberspace to technicians (and the military and intelligence services) risks converting cyberspace into a Hobbesian space of all at war with all.

The point is illustrated about the debate about Huawei´s role in the development and implementation of 5G mobile telephony. Although much of the debate has been about security, in the longer term the more interesting issue may prove to be industrial standards setting. In previous generations of mobile telephony, the international industrial standards were set by US companies, or companies of US allies. 5G, and in particular second phase 5G, focused on the Internet of Things (IoT), is the first time that international industrial standards are being set by a company based in a US rival (China´s Huawei). The myriads of western technical experts and representatives from telecommunications ministries did not understand the security and geopolitical implications of China´s sudden interest in industry standards setting. The US is now trying to regain lost territory. This example has two lessons for cyberdiplomacy: the danger of leaving international technology discussions to technicians, and that such industry standards setting meetings in the future will be ever more geopolitical, and the presence of diplomats ever more important.

Cyberspace

There are multiple definitions of cyberspace, and many are unilluminating. For the purposes of this policy briefing, cyberspace is seen as the internet plus the social actors, devices and technologies connected by it. The last point is important. Increasingly the internet not only links human users, but also devices and machines (Internet of Things) and enhances other technologies (video, artificial intelligence etc). More specifically, we can think of cyberspace having four layers:

- Physical layer: the cables, switching stations, storage facilities and other physical infrastructure on which the internet is built.

- Logic layer: the protocols, codes and root servers which direct the internet and ensure that data arrives where it is intended.
- Data layer: the data content of web pagers, emails and other communications.
- Social level: the users, devices, machines and technologies which interact through the internet.

All four layers are political and geopolitical, and generate problems which go beyond the scope of technicians to solve. At the physical level, the underwater cables are potentially vulnerable to terrorism and geopolitical conflict. At the logic level there are, as we have seen, arguments about the status of ICANN, as well as net neutrality and encryption. At the data level, arguments centre on data protection and webpage content control. At the social level, conflict arise between different state and non-state actors as they seek to manipulate or extract information, or use the internet to coerce other actors.

Internet Agendas

The political and geopolitical debates surrounding cyberspace can be broadly divided into the internet governance and cybersecurity agendas, although they are related and probably best dealt with in a coordinated way. The internet governance agenda focuses on the way the internet is managed as a public good, and tackles issues on all levels of cyberspace. These issues include the status of the physical infrastructure and ICANN, net neutrality, encryption, data protection, regulation of the OTT (Over the Top – the rich tapestry of internet service providers constructed "over the top" of national telecommunications companies), control of "undesirable" content and some criminal activities. State actors tend to divide on these issues between the Free Internet Countries, which seek to avoid national sovereignty in cyberspace, and the Cyber Sovereignty Advocates, which push for the exercise of national sovereignty in cyberspace and placing its regulation within the hands of the UN or some other international organisation. Non-state actors tend to prefer the positions of the Free Internet Countries.

The Cybersecurity Agenda focuses on the use of the internet to penetrate computer systems without the permission of their owner. Such illicit penetration of computer systems can aim at degeneration (causing permanent damage to information systems or through them physical infrastructure – kinetic damage), disruption (the temporary close down of computer systems – often through distributed disruption of service (DDOS) attacks), espionage (the extraction of data without the permission of the owner), or disinformation (the use of the internet to spread disinformation and fake news to undermine political stability). While the number of illicit cyber penetrations is growing significantly every year, there has so far only been one clear case of a degeneration attack (the Stuxnet attack against the Iranian nuclear processing plant at Natanz). Much more common are disruption, espionage and disinformation operations. They are carried out by state and non-state actors, including criminals and terrorist groups. Organised crime groups operating in cyberspace are often associated with state actors, which may use them as surrogates for espionage, disruption or disinformation

operations. State actors often develop cyber strategies combining different kinds of operations, for example an espionage operation to extract information which is then leaked through the internet as part of a disinformation campaign. Alternately state actors, or their criminal surrogates, steal intellectual property which they can later pass to their companies to gain technological advantage.

Key non-state actors in cyberspace are the major internet companies, including social media platforms, search engines and online sales platforms. Social media platforms like Facebook and YouTube and search engines like Google are embroiled in debates about data protection, encryption and disinformation operations. Facebook and Twitter have in particular been singled out for their role in subverting western political processes. Their underlying algorithms not only contribute to advertising revenues, but also to the spread of disinformation and fake news. Online sales platforms raise issues of commercial regulation and taxation (the OTT). Facebook´s proposal to establish its own cryptocurrency the Libra raises significant geopolitical as well as regulatory and criminal issues. States frequently have to rely on private cybersecurity companies to attribute cyberattacks. Even when they do not, pronouncements by such private sector cybersecurity companies on attribution can shape debates about policy responses in ways that governments find hard to avoid. As increasingly important geopolitical actors in their own right, internet companies are also vulnerable to cyber operations seeking to disrupt, steal data or damage their reputations.

International Law in Cyberspace

A key issue is whether international law applies in cyberspace. While some states assert that it does, there is no universal agreement on this. The UN Secretary General set up a Group of Government Experts to seek to agree international norms in cyberspace. Despite repeated meetings they have made limited progress (they have agreed that Cyber Emergency Rescue Teams (CERTs) should be immune from attack). At one point it looked as if they had agreed that international law did apply in cyberspace, but key countries subsequently backed off. Attempts have been made to negotiate specific norms for cyber behaviour, but they have been limited in scope and limited in signatories. For example, the Budapest Convention focuses on collaboration against different forms of cybercrime, but key cyber powers have neither signed nor ratified it. The Tallinn Manual looks at broader cybersecurity issues, but is a NATO document essentially setting out NATO doctrine. A further problem is that those affirming that international law applies in cyberspace tend to be Free Internet Countries. But existing international law is essentially Westphalian, built on the concept of national sovereignty, meaning that the application of international law in cyberspace could serve to undermine their position on the internet governance debate.

A particular issue is the application, or not, of the Law of Armed Conflict (LOAC) to the cybersecurity agenda. Issues like attribution and unintended escalation raise issues in cyberspace that are less serious in physical space. Concepts like neutrality and arms control have limited application to cybersecurity, where negotiations on limitations are more likely to apply to targets than weapons. There are no internationally agreed norms

on what constitutes an armed attack, what constitutes acceptable limits to cyber activity (and what would constitute a cyber casus belli) or whether it is legitimate to respond in physical space to attacks in cyberspace (ie is it legitimate for a state to respond to a serious attack in cyberspace, perhaps causing physical damage, by launching air strikes?). The LOAC as it exists cannot simply be transferred to cyberspace. New norms will need to be negotiated, and will require diplomats to negotiate them.

The Cybersecurity Dilemma

The cyber version of the classic security dilemma suggest that diplomats and diplomacy may be more, rather than less, important in cyberspace. In the cybersecurity dilemma a country, fearful of a cyberattack from a second country, penetrates its computer systems to identify its capabilities and intentions. The second country interprets this as preparation for a cyberattack and so redoubles its penetration of the first country, now also convinced of its bad intentions. The key problem is that a penetration of computer systems to ascertain capabilities and intentions looks exactly the same as a penetration in preparation for a future disruption or degeneration attack. The key in mitigating the cybersecurity dilemma, as it is in unintentional escalation, is to correctly identify the intentions of the other country (or non-state actor). Recent studies suggest that the key to correctly interpreting intentions is regular face to face contact. The profession best placed to maintain regular face-to-face contact with senior policy makers, opinion formers and decision makers in foreign countries is that of the diplomats.

Diplomacy

It is worth spelling out in what the diplomatic approach to managing the security and governance problems generated cyberspace consists. Several elements can be identified, including:

- A willingness to accept “good-enough” outcomes rather than insist on optimal solutions;
- A tendency to manage problems rather than necessarily solve them;
- An analytical approach built around identifying the intentions of “the other”, seeking to understand not only want the other intends, and why, but also how he interprets our intentions;
- The development of global networks of information and influence among both state and non-state actors;
- The constructions of “coalitions of the willing” built on shared preferred outcomes rather than necessarily shared values and ideologies;
- The socialisation of state and non-state actors into an international community;
- A constructivist approach to international law, which recognises that the motivation for state and non-state actors to obey international laws lies in a combination of self-interest, self-perception (and how they want to be perceived by others) and a desire to remain a part of the international community.

Cyberdiplomacy

Diplomats operating in cyberspace will need to perform many of the same functions as in physical space. They will need to be able to analyse the different cyberspace agendas, the place of their country in them and where their countries´ interest lies. They will need to identify the intentions of other actors, both state and non-state, and explore possible areas of agreement which could serve as the building blocks towards agreement on norms of behaviour in cyberspace, both in terms of internet governance and cybersecurity. In doing so, they will focus not so much on shared ideologies or values, but shared preferred outcomes. Developing thick diplomatic networks with state and non-state actors will be essential to the confidence in the identification of their intentions essential to mitigating the cybersecurity dilemma and managing crises in cyberspace. In particular this traditional capacity of diplomats for reliable identification of intentions will be central to the attribution of cyberattacks (complementing technical attribution through cyber forensics) and managing escalation in the case of cyberattacks with unintended consequences.

Top-down regulation through international agreements and organisations is unlikely to be effective in building internet governance, not least because of the role of non-state actors. Norms of behaviour in cyberspace, whether for internet governance or cybersecurity, are more likely to be bottom-up and involving a broad range of state and non-state actors. The model is likely to be that of the Paris Accords on Climate Change. Existing International Law cannot be applied wholesale to cyberspace. Rather a new cyber international law will be constructed progressively and over time (as indeed was international law in physical space). Diplomats will be the main government actors in this task, engaging with the different state and non-state actors, identifying the preferred outcomes they share and constructing coalitions around these. They will aim not at optimal solutions, but rather acceptable ways of managing the problems. New technologies like blockchain will enable the progressive building blocks of norms of behaviour in cyberspace to be recorded reliably. The international lawyers can write it up afterwards. This process of progressive construction of rules of the game for cyberspace, whether for internet governance or cybersecurity, will require diplomats and their foreign ministries to enhance their capacity for multi-stakeholder diplomacy, the ability to engage with a broad range of state and non-state actors at the same time.

Despite the growing importance of non-state actors, governments and their representatives will remain crucial to managing cyberspace. In many ways the international environment in cyberspace is moving away from the Free Internet Nations towards the Cyber Sovereignty Advocates. Even some of the Free Internet Nations are limiting their enthusiasm for a “free internet”, with the US abandoning net neutrality and increasing concerns in Europe about data protection and unacceptable content. Moreover, it is state actors who have the greatest cyberattack capacity, and the greatest capacity to use cyber to inflict kinetic damage on rivals. Although there has so far been only one clear example of a degeneration attack, this may reflect the lack of conflict in physical space between those states with the most sophisticated cyber capabilities.

States have used disruption and disinformation attacks in attempts to destabilise rivals. Diplomats will have to manage these inter-state relations and conflicts in cyberspace as they do in physical space. Strategic responses to disinformation and disruption operations will need to include the diplomatic element, as well as public diplomacy and strategic communications. Diplomats will need to try to socialise the broad range of state and non-state actors into an international cyber community, where the desire to remain seen as a member of that community constrains behaviour. They will also need to make clear the costs of not being a member of that community. Ministries of Defence have already incorporated cyber in their national security strategies. Ministries of Foreign Affairs must do the same, bringing cyberdiplomacy to the heart of foreign policy and their strategies for achieving it, and ensuring that their diplomats have the knowledge and skill sets to carry out their functions.

Conclusion

Cyberspace is too important to leave to technicians or intelligence services. The key problems arising in cyberspace are political and geopolitical. Diplomats were slow to understand the importance of digital technologies. To a large extent they have focused almost exclusively on the use of digital technologies to promote broader diplomatic agendas, and in particular the use of social media as a tool for public diplomacy and national promotion. They have paid far less attention to the implications of these digital technologies for geopolitics and international relations. If they continue to ignore the diplomacy of cyberspace, they increase the danger of cyberspace become an arena of Hobbesian war of all on all. Diplomats need to engage with the politics and geopolitics of cyberspace, contributing to the construction of norms and rules of the game for cyber behaviour. Rather than being left to Ministries of Telecommunications or Cybersecurity commands, the political and geopolitical implications of cyberspace need to be brought to the heart of foreign policy making.

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 Eastern 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).