T20
SAUDI ARABIA 2020
THINK

POLICY BRIEF

THE CYBER DIPLOMACY OF CONSTRUCTING NORMS IN CYBERSPACE

Task Force 5

THE FUTURE OF MULTILATERALISM AND GLOBAL GOVERNANCE

Authors

MARIO TORRES, SHAUN RIORDAN

موجز السياسة

الدبلوماسية السيبرانية لصياغة القواعد في الفضاء السيبراني

فريق العمل الخامس

مستقبل التعددية والحوكمة العالمية

المؤلفون

ماريو توريس، شون ريوردان

ABSTRACT

The Group of 20 (G20) should support the formulation of acceptable behavior norms in cyberspace. The G20 should 1) create a working group to explore the lessons from the Paris Agreement process for developing effective multi-stakeholder cyber diplomacy, 2) develop capacity-building programs in cyber diplomacy for state and non-state actors, 3) create a working group to explore how digital technologies can support the implementation of cyber diplomacy, both by state and non-state actors, 4) create a working group to explore the specific issue of international industrial standards setting and how this can be de-politicized to ensure common global standards for future technologies, and 5) appoint an ambassador to the technology sector.

ينبغي لمجموعة العشرين أن تدعم صياغة قواعد سلوكية مقبولة في الفضاء السيبراني. حيث تقوم مجموعة العشرين بالآتي: 1ـ إنشاء مجموعة عمل لاستكشاف الدروس من عملية اتفاقية باريس لإعداد دبلوماسية سيبرانية فعَّالة لأصحاب المصلحة المتعددين، 2ـ تطوير برامج بناء القدرات في مجال الدبلوماسية السيبرانية للجهات الفاعلة الحكومية وغير الحكومية. 3ـ إنشاء مجموعة عمل لاستكشاف كيف يمكن للتقنيات الرقمية أن تدعم تطبيق الدبلوماسية السيبرانية من قبل الجهات الفاعلة الحكومية وغير الحكومية على حدٍّ سواء. 4ـ إنشاء مجموعة عمل لاستكشاف قضية محددة وهي وضع المعايير الصناعية الدولية، وكيف يمكن نزع الطابع السياسي عن هذا الأمر من أجل ضمان معايير عالمية مشتركة للتقنيات المستقبلية. 5ـ تعيين سفيرٍ لقطاع التكنولوجيا.

CHALLENGE

Although the United Nations General Assembly (UNGA) has agreed that International Law, and in particular the UN Charter, apply to cyberspace, there is no general consensus about what this implies. In 2004, the secretary-general of the UN set up the Group of Government Experts to examine establishing behavioral norms within the context of the First Committee, excluding issues such as espionage, Internet governance, and digital privacy. It has thus far reached only limited conclusions. In 2018, the UNGA set up a separate process, the Open-Ended Working Group (OEWG), with membership open to any UN member and a broader remit. Although the OEWG allows some participation by non-state actors, membership remains limited to UN member states. Both working groups are hampered by disagreements among permanent members of the Security Council. It seems unlikely that either group will make substantial progress in the near future (Riordan 2019a).

However, establishing behavioral norms in cyberspace is an urgent task. The ambiguities inherent in cyberspace surrounding attribution, identification of intentions, or the nature of cyber operations generate uncertainties that increase risks of escalation. Without clear guidance on what is regarded as acceptable behavior, state actors are less certain about the red lines of their rivals (Kello 2017). What constitutes proportional response is contested. The uncertainties extend beyond inter-state conflict to areas such as Internet governance, economic and commercial regulation, and cybercrime. The conflict over the presence of different companies in 5G networks illustrates the risk of politicizing international industrial standard setting meetings to the disadvantage of less digitally advanced countries.

Individual states and regional groups are resorting to unilateral measures to give the extra-territorial effect (e.g. the European Union´s General Data Protection Regulation). However, this dynamic creates the risk of rules being set by economically powerful states to the exclusion of others. Non-state Internet users and suppliers are also excluded. The multi-stakeholder nature of the Internet is reflected in the Internet Corporation for Assigning Names and Numbers but is not reflected in current efforts to establish broader norms of behavior in the UN’s system. This not only elevates the interests of states over those of Internet users but ignores the powerful Internet companies and social media platforms (Libicki 2016).

Securing the acquiescence of major cyber powers to such international behavioral norms will not be easy. However, something similar to what exists in physical space should be attempted: a broadly accepted, if not always respected, body of behavioral norms that offer guidance to state and non-state actors (Buchanan 2017). The COVID-19 outbreak has demonstrated the urgency of this issue. Lockdowns have made societies more dependent on digital technologies and more vulnerable to cyberattack and disinformation operations. Even critical infrastructure, such as hospitals, have not been immune to cyberattacks during the crisis. Cyberespionage appears to have been used to steal secrets about possible vaccines and treatments for the disease. The development of applications for tracing patterns of contagion and the evolution of pandemic diseases require international rules of good practice.

PROPOSAL

The various UN approaches to establishing behavioral norms in cyberspace are hampered by the renewed paralysis in the Security Council. Limiting the debate to states excludes key non-state actors and subordinates broader civil society interests to geopolitical considerations. A new approach that reflects the multi-stakeholder nature of cyberspace and bypasses geopolitical conflicts through progressive construction of norms from bottom-up is required. The model should be the Paris Agreement on climate change. The final agreements were governmental, but the road toward them was built from heterogenous networks of state and non-state actors (Riordan 2019b).

The G20 should promote a new multi-stakeholder cyber diplomacy to develop alternative approaches to reaching an agreement on behavioral norms in cyberspace. The G20 should support capacity building in cyber diplomacy among both state and non-state actors. It should help state and non-state actors to identify shared preferred outcomes, based on which norms of acceptable behavior in cyberspace can be constructed. This new cyber diplomacy will need to take full advantage of new technologies in promoting a wide range of engagements between state and non-state actors. These should extend beyond the current use of social media platforms as tools for public diplomacy. Finally, the G20 needs to develop cyber diplomacy as a practical tool for de-escalating conflicts over new technologies and, in particular, mitigating the risks associated with the increasing politicization of industrial standards setting.

Specifically, the G20 should:

- Create a working group consisting of both state and non-state actors to analyze the Paris Agreement on climate change and the lessons for a new approach to establishing behavioral norms in cyberspace. The working group should focus on the role of scientists (technicians) in promoting understanding of the underlying scientific (technical) issues, the interaction between different non-state actors (e.g. non-governmental organizations and corporations) and the construction of heterogenous “coalitions of the willing” built around preferred shared outcomes. The working group should report the potential of a new inclusive model for constructing international behavioral norms in a world where the Security Council is frozen by geopolitical conflict, particularly for cyberspace.

- Encourage states to place the development of global norms of cyber behavior at the center of their foreign policy and actively develop multi-stakeholder cyber diplomacy. As a part of this, the G20 should develop capacity-building workshops to support state and non-state actors in the development of cyber diplomacy capacity. This is especially important for those state and non-state actors that have until now been largely excluded from the debates on international Internet governance. The capacity-building workshops should focus on understanding the issues of Internet governance and cybersecurity agendas and developing a multi-stakeholder diplomacy capable of engaging with a broad range of state and non-state actors (Valeriano, Jensen and Maness 2018). Such a diplomacy should make effective use of digital technologies and online platforms to extend diplomatic reach and compensate for the relative lack of diplomatic resources. Capacity-building workshops should be made available to both state and non-states actors.

- Establish a working group to explore how digital and other technologies can be developed to support a cyber diplomacy approach to regulate state and non-state behavior in cyberspace. In effect, this working group will focus on the process rather than the content of cyber diplomacy. That is, how digital and other technologies can be better used to engage with state and non-state actors to build like-minded coalitions and construct agreed upon behavioral norms. Key issues will include the use of online platforms for scenario building and simulations; the use of social media platforms as networking as well as public diplomacy tools; the use of platforms such as Zoom for online workshops and conferences; the use of blockchain technologies to record localized agreements as building blocks in constructing wider norms; and the use of computer games to encourage engagement and explore possible agreements, especially with younger generations. The working group should also engage with Internet and technology companies to discuss what further developments in technology may be available for diplomacy in the future. It should explore the possible development of platforms tailor-made to promote cyber diplomacy strategies. Such engagement with Internet and computer companies will also help entangle them in the process of constructing behavioral norms in cyberspace (in part by treating them as geopolitical actors in their own right).

- Establish a working group to explore the specific issue of international industrial standards setting. The controversy over the participation of certain companies in 5G mobile networks relates not only to security concerns, but also to the role of those companies in setting international industrial standards for 5G technologies. Industrial standard setting meetings for new technologies threaten to become geopolitical battlegrounds, undermining the universality of the standards for these technologies. Emerging and less technologically developed countries will be most impacted by this fragmentation of international standards. The G20 working group should explore how this politicization of international industrial standards can be avoided, and how global standards can be maintained in the future. In doing so, the group should work closely with the other two working groups proposed in this policy briefing, informing their work and benefiting from their conclusions.

- Appoint an ambassador to the technology sector. A tech ambassador would represent the G20 in discussions with the major Internet and technology companies and search engines. The tech ambassador's remit would include (1) conveying the interests of G20 members to the technology companies, (2) engaging with them over key Internet governance and cybersecurity issues (privacy, disinformation, attribution, cyberattacks, cybercrime), and (3) ensuring they understand their responsibilities and the geopolitical implications of their actions and their role as, effectively, geopolitical actors in their own right. The ambassador should encourage them to participate in key cyber diplomacy debates and engage with other, smaller, state and non-state actors. The ambassador would seek to represent the interests of countries in the global south who are less able to influence major Internet companies. Through their engagement with the tech sector, the ambassador would seek to identify and report back to the G20 on the key political and geopolitical implications of future technologies, allowing diplomacy, for once, to get ahead of the technological curve. The tech ambassador´s office should include people with both diplomatic and technical backgrounds.

In 2017, Denmark appointed an ambassador to the tech sector, with offices in Silicon Valley , Copenhagen, and Beijing (Torres and Riordan 2019). His remit included promoting Denmark´s interests in the tech sector (including Denmark as a destination for tech investment) and engaging with the tech sector over key political issues. The world has moved on since then. Major Internet and social media companies and search engines are playing an ever more important role in international relations, whether as facilitators of disinformation or (potentially) providers of global digital currencies. The US Internet giants are being joined by companies from other countries. COVID-19 has only increased their importance, as more companies and governments are forced to function online. In many respects, they have become geopolitical actors in their own right. The G20 is uniquely placed to engage with them because its broad range of membership implies it can speak on behalf of the global south, which, too often, has no voice in these debates, as well as those better placed.

Uncertainty in cyberspace is likely to continue rising, both because of the increasing complexity of cyberspace itself and the instability of the geopolitical actors operating through it (Kello 2017). Non-state actors, such as Internet companies and social media platforms, add to the level of uncertainty. This causes discomfort for many policy makers, as well as technicians, who are accustomed to making decisions with complete knowledge and under stable conditions (Sharp 2009). However, diplomats are used to uncertainty and making decisions with incomplete knowledge. Their approach to managing international problems makes them well equipped for constructing cyberspace norms. They can empathize with others´ views, socialize with an international community of diplomats, engage in frequent in-person discussions, and settle for acceptable outcomes rather than optimal solutions. They need to move cyberspace to the center of their agendas (Holmes 2018). However, just diplomats are not enough. Rather, a broad range of stakeholders, both state and non-state, must be included to develop new approaches to the formulation of norms, no longer dependent on top-down international organizations. The G20, which is itself an innovative reaction to a previous crisis, should be well-placed to lead this process.

Conclusion

Top-down approaches to establishing behavioral norms in cyberspace have so far had limited success, having attempted too much too quickly. They have been more reactive, only following major traumas. The current confrontations between the permanent members in the Security Council make the UN an unlikely path for generating new behavioral norms in any domain (Stuenkel 2016). This policy brief recommends that the G20 should support an alternative progressive bottom-up approach through the development of a multi-stakeholder cyber diplomacy. The broader membership of the G20 makes it hard for any one state to dominate, while being less unwieldy than the UNGA. In particular, the G20 should appoint an ambassador to the tech sector to ensure that Internet and tech companies understand the concerns of the global south as well as the north. The geopolitical environment that seems to be developing following the COVID-19 outbreak will not make this easy. However, the outbreak itself, through both increasing our dependence on digital networks and exposing their vulnerabilities, has made the task more urgent.

Relevance to G20

A stable cyberspace ruled by universally agreed norms is key to developing the inclusive economy that the G20 promotes. Global economic growth and financial stability are vulnerable to a whole range of Internet governance and cybersecurity issues. While other fora have focused on the commercial, security, or criminal governance of cyberspace, the G20 is uniquely placed to tackle the broad range of these issues. This includes the views and interests of small states as well as the cyberspace powers.

Disclaimer

This policy brief was developed and written by the authors and has undergone a peer review process. The views and opinions expressed in this policy brief are those of the authors and do not necessarily reflect the official policy or position of the authors' organizations or the T20 Secretariat.

REFERENCES

Buchanan, Ben. 2017. The Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System. London: C. Hurst.

Holmes, Marcus. 2018. Face-to-Face Diplomacy: Social Neuroscience and International Relations. Cambridge: Cambridge University Press.

Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press.

Libicki, Martin C. 2016. Cyberspace in Peace and War. Annapolis: Naval Institute Press.

Riordan, Shaun. 2019a. Cyberdiplomacy: Managing Security and Governance Online. Cambridge: Polity.

Riordan, Shaun. 2019b. The Geopolitics of Cyberspace: A Diplomatic Perspective. The Hague: Brill.

Sharp, Paul. 2009. Diplomatic Theory of Diplomatic Relations. Cambridge: Cambridge University Press.

Stuenkel, Oliver. 2016. Post-Western World. Cambridge: Polity.

Torres, Mario and Shaun Riordan. 2019. Techplomacy and the Tech Ambassador. Salamanca: IEEI.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. 2018. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford: Oxford University Press.

AUTHORS

Mario Torres
Pontifical University of Salamanca

Shaun Riordan
European Institute for International Studies

t20saudiarabia.org.sa