2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms

Nikola Pijović
Cyber Security Cooperative Research Centre Postdoctoral Research Fellow
School of Politics and International Relations / Law School
University of Adelaide, Australia
nikola.pijovic@adelaide.edu.au

Abstract: The development of global norms of responsible state behaviour in cyberspace has, over the past decade, become a significant foreign policy issue and a new battleground between states. The contested and competitive nature of global cyberspace norm building suggests that although there are complicated legal and technical issues at play, the development of cyberspace norms remains primarily a contestation of values, ideologies, and strategic interests. This paper argues that the competition to shape the governance of cyberspace through the development of cyberspace norms represents a continuation of foreign and strategic policy applied to the cyber domain. This has resulted in a growing cyberspace 'Great Game' between the Five Eyes alliance countries (the United States, United Kingdom, Australia, Canada, and New Zealand) and the Sino-Russian bloc (China and Russia). The Five Eyes and the Sino-Russian bloc are key cyber powers and cyberspace norm entrepreneurs whose leadership is instrumental in promoting global cyberspace norm preferences. However, each camp advocates a set of norm preferences inherently at odds with the other's, which has resulted in growing competition for dominance in cyberspace norm prescription and promotion. The paper outlines the key cyberspace norm proposals and initiatives promoted by the Five Eyes and the Sino-Russian bloc, discussing their main differences. It argues that the latest round (2019–2021) of the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace (UNGGE) deliberations is unlikely to help bridge these differences in any substantive way. The cyberspace 'Great Game' and the increasingly competitive nature of cyberspace norm development will remain a feature of global efforts to govern cyberspace throughout the 2020s.

Keywords: *Five Eyes, cyberspace norms, China, Russia, cyber security*

1. INTRODUCTION[1]

The governance of cyberspace and development of global norms of responsible state behaviour have, over the past decade, become significant international relations issues. Although the decade of the 2000s saw limited efforts aimed at international agreement over the governance of cyberspace, the 2010s have seen a proliferation of global cyberspace norms (Barrinha and Renard 2020, 764). However, the contested and competitive nature of global cyberspace norm building suggests that although there are complicated legal and technical issues at play, the development of cyberspace norms remains inherently a contestation of values, ideologies, and interests. Echoing Carl von Clausewitz's (2007, 28) famous maxim that war 'is merely the continuation of policy by other means', this paper argues that notwithstanding the novelty of the cyber domain, the development of cyberspace norms is merely a continuation of foreign and strategic policy by other means. This continuation of foreign and strategic policy has resulted in a cyberspace 'Great Game' between the Five Eyes alliance (the United States [US], United Kingdom [UK], Australia, Canada, and New Zealand) and the Sino-Russian bloc (China and Russia). The Five Eyes and the Sino-Russian bloc compete for dominance in cyberspace norm prescription, with each side advocating a set of norm preferences incompatible with the other's. While these norm preferences are also advocated by, and find varying degrees of support in, many other states, the Five Eyes and the Sino-Russian bloc merit special attention as key global cyber powers and norm entrepreneurs whose leadership is instrumental in promoting and adhering to global cyberspace norm preferences.[2]

The paper first provides brief background on the Five Eyes and the Sino-Russian bloc as global cyber powers. It then examines their competing cyberspace norm preferences and norm building initiatives. The focus is on critically analysing the fundamental differences underpinning each side's differing conceptions of what global cyberspace norms should promote: 'cyber security' versus 'information security', 'multi-

[1] The work has been supported by the Cyber Security Research Centre Limited, whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

[2] These states are not the only globally relevant cyber powers, but they rank among the top 10 most cyber powerful nations and have the most advanced abilities to 'conduct aggressive cyber operations (or to deter or withstand such operations)', 'influence the international cyber agenda', and use cyber tools to 'promote a broader agenda and wider interests' (Barrinha and Renard 2020, 755). For cyber power rankings, see Voo et al. (2020), 8.

stakeholder' versus 'multilateral' governance of the internet, and 'transnationalism' versus 'cyber sovereignty'. The conclusion highlights the implications of the cyberspace 'Great Game' for the future of cyberspace norm development.

2. THE FIVE EYES AND THE SINO-RUSSIAN BLOC AS KEY CYBERSPACE POWERS

In the original 'Great Game', the British and the Russians competed for influence in Central Asia throughout the 19th century. In the cyberspace 'Great Game', the British and the Russians, in addition to other key cyber powers such as the US and China, compete over how the world governs cyberspace. As in the original 'Great Game', there is no overt military confrontation (yet), but unlike the original 'Great Game', the fallout of the cyberspace one is truly global in reach. For example, as the Five Eyes countries have moved to effectively ban the Chinese company Huawei from participating in the construction of their 5G mobile technology infrastructure (Slezak and Bogle 2018; Trump 2019; Tobin 2019; Gold 2020; Duckett 2020), international economists have warned that the ban poses a significant threat to the stability and growth of the global economy (Moon and Bray 2019). Although this ban has been discussed primarily in terms of national security (could the Chinese government use Huawei's technology for spying purposes?), it is fundamentally underpinned by the contestation of ideas about the governance of cyberspace and norms of responsible state behaviour. Given that 5G technology is the future of cyberspace and global connectivity and the world is – especially as a result of the COVID-19 pandemic – increasingly dependent on information and communications technology (ICT), the Huawei story aptly highlights the global significance of the cyberspace 'Great Game'. Therefore, while there are many differences between the original 'Great Game' and the one now played in cyberspace, the comparison points out the highly competitive nature of the global governance of cyberspace.

The Five Eyes are made up of the US, UK, Australia, Canada, and New Zealand, united 'by the language, values and institutions associated with the historical experience' of Britain's empire (Vucetic 2010, 456). This grouping is also referred to as the 'Anglosphere' (Wellings and Mycock 2019). Although not a 'unitary actor' in global affairs, the Anglosphere continues to 'define, order and promote' the values, policies, and transnational institutions that underpin the current rules-based international order (Vucetic 2010, 469). This is mainly due to the Five Eyes' success in fashioning the post-World War II global order, whereby 'a global society hitherto dominated by a system of states and empires received an important layer of multilateral institutions designed mostly by, and for, the Anglo-American elites' (Vucetic 2010, 468).

However, the close relations between the Five Eyes are today underpinned by more than just a shared history and ability to shape global power dynamics. They are underpinned by a closely aligned strategic interest, especially vis-à-vis China, and an ever-growing web of Five Eyes 'policy networks' that 'have been central to the co-production of policy, collaboration in shared policy problems and the transfer of policy ideas and practices' between these countries (Legrand 2019, 66). The Five Eyes alliance itself was established by the 1946 British-US Communication Intelligence Agreement (UKUSA), updated in 1955 and expanded to include Australia, Canada, and New Zealand (NSACSS n.d.).[3] Today, the Five Eyes constitute 'a cooperative, complex network of linked autonomous intelligence agencies' where 'individual intelligence organizations follow their own nationally legislated mandates, but interact with an affinity strengthened by their common Anglo-Saxon culture, accepted liberal democratic values and complementary national interests, all seasoned with a profound sense of confidence in each other and a degree of professional trust so strong as to be unique in the world' (Cox 2012).

Cyber security is of critical importance for the Five Eyes alliance, with the original UKUSA Agreement founded on the sharing of 'communications intelligence' – today's 'signals intelligence' (SIGINT). The continued centrality of SIGINT sharing to the Five Eyes alliance is reflected in the fact that the core Five Eyes intelligence agencies remain SIGINT and cryptology agencies: the National Security Agency (US), the Government Communications Headquarters (UK), the Australian Signals Directorate (AUS), the Communications Security Establishment (CAN), and the Government Communications Security Bureau (NZ) (Richelson 2016, 370). The Five Eyes countries enjoy some of the highest internet usage rates globally; their economies are increasingly digital and therefore significantly exposed to the benefits and perils of cyberspace (especially in the COVID-19 pandemic environment); and their national security infrastructure and governance systems are overwhelmingly reliant on ICT – all clear reasons why cyber security holds critical importance (GCDL n.d.).

China and Russia also rank among the world's strongest cyber powers. In the past two decades they have developed a clear strategic closeness, largely motivated by concerns over the West's (and especially the Five Eyes') promotion of global political and economic liberalism in the post-Cold War period (Bolt and Cross 2018; Lukin 2018). This unity of purpose in contesting many of the values, policies, and norms associated with global liberalism is especially evident with regards to the governance of cyberspace. China's cyber strategy is underpinned by a fundamental focus on cyber sovereignty, exhibited in three key goals: limiting the threat of the internet to the Communist Party's hold on power; shaping global cyberspace norms to extend China's political, military, and economic influence; and countering Five Eyes advantages in cyberspace (Segal 2017, 1). While appreciation of cyber sovereignty is, to varying

[3] The actual term 'Five Eyes' refers to a dissemination caveat of intelligence products ('Secret/Top Secret – AUS/CAN/NZ/UK/US Eyes Only') shortened by practitioners in everyday use. See Cox (2012).

degrees, shared by all states (including the Five Eyes), the primacy of sovereignty in China's 'cyber diplomacy' has become a significant point of contestation with the Five Eyes, who advocate for a more open and transnational cyberspace. In the past decade, China's cyber security policy has consistently highlighted sovereignty as a key concern, with its 2016 *National Cyberspace Security Strategy* (CCM 2016) and 2017 *International Strategy for Cooperation in Cyberspace* (MFAPRC 2017) ranking sovereignty as a first principle and strategic objective.

Russia's cyber strategy is underpinned by the concept of 'information warfare', with a preference for the term 'information security' (a preference shared by China). The Russians define information warfare as '…the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems', constituting 'a massive psychological manipulation of the population to destabilize the state and society' and compelling 'the state to take decisions for the benefit of the opposing force' (Lilly and Cheravitch 2020, 133). Russia's strategic thinking on information/cyber security continues to be dominated by the idea of information warfare and supremacy, with a particular concern about foreign interference (Lilly and Cheravitch 2020, 134–136). These concerns are generally shared by China and motivate both countries to promote global cyberspace norms they hope will advance their interests and constrain the Five Eyes' cyber dominance. While there are many differences between China and Russia's cyber security experiences (Whyte and Mazanec 2019, 232), their primary concern over political stability and foreign interference is a key factor underpinning their cooperation on the development of global cyberspace norms.

3. HOW THE FIVE EYES AND THE SINO-RUSSIAN BLOC ARE SHAPING THE GOVERNANCE OF CYBERSPACE

Since the early years of the 21st century, the Five Eyes and the Sino-Russian bloc have played prominent roles in trying to shape how cyberspace is governed. Although they have been able to nominally agree that existing international law applies to the cyber domain, the two blocs hold inherently incompatible cyberspace norm preferences. Their contestation of ideas on how cyberspace should be governed is underpinned by fundamental ideological differences in conceptualizing cyber security and the political values each bloc promotes in an effort to advance their strategic interests. Before examining their differing visions for the governance of cyberspace, it is worth briefly reiterating what the two blocs have been able to at least nominally agree on. In this context, the paper examines their contributions to the most prominent global forum discussing the governance of cyberspace: the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace (formerly, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security) (UNGGE).[4]

There have been six UNGGE sessions: 2004–2005, 2009–2010, 2012–2013, 2014–2015, 2016–2017, and 2019–2021 (currently still underway). Reports are produced by consensus, with the whole group having to 'agree upon the report in its entirety' before making it public, and this implies at least nominal (if not always substantive) agreement (UNIDIR 2016, 5). The first UNGGE (2004–2005) failed to reach a consensus report, with differences arising over 'how to characterize the threat posed by State exploitation of ICTs for military purposes' and 'whether the discussion of ICT security should focus solely on the ICT infrastructure or include information content as well' (UNIDIR 2016, 6). The second UNGGE (2009–2010) produced a report which expressed its concern about states 'developing ICTs as instruments of warfare and intelligence, and for political purposes', recommending 'further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure' (UN A/Res/65/201 [2010], 2, 8). The third UNGGE (2012–2013) agreed that 'international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'. It also concluded that state sovereignty applies in cyberspace, that 'state efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments', and that states 'must meet their international obligations regarding internationally wrongful acts attributable to them', 'must not use proxies to commit internationally wrongful acts', and 'should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs' (UN A/Res/68/98 [2013], 8). The fourth UNGGE (2014–2015) reiterated the same points made in the third session, adding that states had 'jurisdiction over the ICT infrastructure located within their territory' and that 'the accusations of organizing and implementing wrongful acts brought against States should be substantiated' (UN A/Res/70/174 [2015], 12, 13).

The fifth UNGGE (2016–2017) was to expand on the question of 'how' international law applied to norms of responsible state behaviour but was unable to find agreement. It failed to provide a consensus report for various political and ideological reasons, confirming 'that there are significant differences of opinion' between states 'on how to apply international law' to their use of ICTs, and that the most visible and sensitive contestation is related to questions of 'state sovereignty versus international obligations, and the relationship between the State and the individual' (Tikk and Kerttunen 2017, 15). The divisions were familiar: between the 'Western or "like-

[4] China, Russia, the UK, and the US are permanent members of the UNGGE. Australia was a member in 2012–2013, 2016–2017, and 2019–2021, and Canada in 2012–2013, 2014–2015, and 2016–2017.

minded" approach that focuses on promoting and explaining' existing international law's applicability to cyberspace, and the Sino-Russian 'call for *lex specialis*' to govern cyberspace and 'reinforced international political structures, mainly the UN, as the mechanism to maintain international peace and security' (Tikk and Kerttunen 2017, 15–16). As of the writing of this paper, it is unclear if the sixth UNGGE (2019–2021) will produce a consensus report.

To sum up, the UNGGE process has been able to establish at least some basic principles on the applicability of international law to cyberspace, which can serve as a starting point for global cyberspace norm building. However, these broad categories of international law – often subject to differing and competing interpretations – allow both the Five Eyes and the Sino-Russian bloc to claim legitimacy for their respective cyberspace norm preferences as embedded in international law.

A. The Five Eyes' cyber security norm preferences

The Five Eyes have collectively published 16 national cyber security strategy documents,[5] and although only the ones published in the past decade focus substantively on cyberspace norms, this body of documents clearly indicates Five Eyes cyberspace norm preferences. The May 2011 US *International Strategy for Cyberspace* was the first Five Eyes cyber strategy to outline a clear position on norms of responsible state behaviour in cyberspace. The goal was to 'promote an open, interoperable, secure, and reliable information and communications infrastructure' by building an environment 'in which norms of responsible behaviour guide states' actions… and support the rule of law in cyberspace' (US 2011, 8). The key principles outlined included upholding fundamental freedoms like association and expression; respect for intellectual property and copyright; online privacy and the protection from arbitrary or unlawful state interference with citizens' use of the internet; protection from cyber crime; support for a multi-stakeholder management of the internet; and the right to self-defence by 'all necessary means' (which may be triggered by aggressive malicious acts in cyberspace) (US 2011, 10–14). These principles still form the core Five Eyes cyberspace norm preferences.

In November 2011, the British government published *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, discussing 'rules of the road' for state behaviour in cyberspace. The UK's position was that 'all governments must act proportionately in cyberspace and in accordance with national and international law', including 'respect for intellectual property' and 'fundamental human rights to freedom of expression and association' (Cabinet Office 2011, 27). Australia's 2016 *Cyber Security Strategy: Enabling Innovation, Growth & Prosperity* advocated 'an open, free and secure Internet based on our values of freedom of speech, right to privacy and rule of law' and a preference for multi-stakeholder governance of the

[5] This excludes 'departmental' cyber security strategies published by the US Department of Defence, Department of Homeland Security, etc.

internet, with the fundamental belief that 'state behaviour in cyberspace is governed by international law' (Commonwealth of Australia 2016, 41). The UK's *National Cyber Security Strategy 2016–2021* also promoted 'the application of international law in cyberspace' as well as 'the agreement of voluntary, non-binding norms of responsible state behaviour' (Cabinet Office 2016, 49). In 2017, Australia published its own *International Cyber Engagement Strategy*, outlining Australia's understanding of international law's applicability to 'state conduct in cyberspace' (mostly based on the 2012–2013 UNGGE report) and the country's position on norms of responsible state behaviour in cyberspace (mostly based on the 2014–2015 UNGGE report) (DFAT 2017, 90–94).

In May 2018, the UK outlined its understanding of international law's applicability to cyberspace through a speech delivered by its attorney general (Wright 2018). It specifically highlighted the importance of the UN Charter and Article 2(7) (prohibiting interventions in the domestic affairs of states), Article 2(4) (prohibiting 'the threat or use of force against the territorial independence or political integrity of any state'), and Article 51 (the right to self-defence if cyber operations result in or present an imminent threat of 'death and destruction on an equivalent scale to an armed attack'). On foreign interference, the speech argued that if hostile states used cyber operations 'to manipulate the electoral system to alter the results of an election' or intervened 'in the fundamental operation of Parliament' or the stability of financial systems, that would 'surely be a breach of the prohibition on intervention in the domestic affairs of states'. In the context of the cyberspace 'Great Game', it is hardly surprising that the examples of foreign interference used by the attorney general described the kinds of activities Russia and China have been regularly accused of undertaking in Five Eyes countries (DHS 2016; Packham 2019). Finally, and rather controversially given Sino-Russian concerns over the militarization of cyberspace, the speech argued that 'each state has the right to develop a sovereign offensive cyber capability', which would not, however, imply the militarization of cyberspace because states had 'an obligation' to ensure such capabilities were used 'in accordance with international law' (Wright 2018).

As well as shaping the governance of cyberspace through inputs into the UNGGE, the Five Eyes also promote several highly prominent norm building initiatives they helped establish: the Council of Europe's *Convention on Cybercrime* (the Budapest Convention), the North Atlantic Treaty Organization (NATO)'s Cooperative Cyber Defence Centre of Excellence (CCDCOE), the Global Conference on Cyberspace and the Global Commission on the Stability of Cyberspace (GCSC), and the Freedom Online Coalition (FOC).

The Budapest Convention is arguably the most prominent international treaty outlining specific practices for combating transnational cyber crime (Council of Europe n.d.). All Five Eyes countries aside from New Zealand[6] are parties to it and regularly promote its virtues in fighting cyber crime. While the Convention's stipulation on trans-border access to data without the need to consult national governments (Article 32) provides for a transnationalism in line with Five Eyes cyberspace norm preferences, it clashes with the Sino-Russian preference for cyber sovereignty (China and Russia are not parties to the Convention).

NATO CCDCOE is best known for publishing the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, which is promoted as the 'most comprehensive analysis on how existing international law applies to cyberspace' (CCDCOE n.d.). While the manual does 'not reflect official NATO opinion', it is sponsored by NATO, the US Cyber Command, and the International Committee of the Red Cross and generally underpins the Five Eyes' promotion of the applicability of existing international law in cyberspace (Whyte and Mazanec 2019, 255).

The Global Conference on Cyberspace, which grew out of the 2011 London Conference on Cyberspace, currently represents one of the most prominent international cyber security forums (Cabinet Office 2011, 27). It has produced the 2013 *Seoul Framework for and Commitment to an Open and Secure Cyberspace*, a set of cyberspace norm preferences favoured by the Five Eyes and like-minded states. The Framework promotes international law's applicability to cyberspace, respect for human rights online, multi-stakeholder management of the internet, and for states to 'meet their international obligations regarding internationally wrongful acts attributable to them' (Seoul Framework 2013). The 2015 Global Conference on Cyberspace led to the formation of the Global Commission on the Stability of Cyberspace (GCSC), which in 2019 published its own set of cyberspace norms, promoting the 'integrity of the public core of the Internet' and proscribing foreign interference in 'elections, referenda or plebiscites' (GCSC 2019, 8–9). While the Global Conference on Cyberspace and the GCSC are made up of international delegates and commissioners, the Sino-Russian bloc perceives these two initiatives as dominated by the Five Eyes and like-minded Western states (Segal 2017, 8–9). Therefore, in 2014 China inaugurated its own international forum for promoting Sino-Russian cyberspace norm preferences, the World Internet Conference (World Internet Conference n.d.).

Finally, the Freedom Online Coalition (FOC), whose membership is almost exclusively Western and European, is 'committed to advancing internet freedom – free expression, association, assembly, and privacy online – worldwide' (FOC n.d.). It holds regular conferences, as well as meetings at the margins of UN cyber-dedicated

[6] The New Zealand government has received legislative advice to become a party to the Budapest Convention or to amend existing national legislation to be in line with it. See New Zealand Law Commission and Ministry of Justice 2015, 28, 190, 207–210, 261–264.

fora, and is regularly promoted by Five Eyes countries (New Zealand Government 2015, 10; Commonwealth of Australia 2016, 40–41; US 2018, 11, 25). The FOC has also launched a Digital Defenders Partnership (DDP) to 'protect critical Internet users' like 'human rights defenders' (activists, bloggers, civil society organisations, and journalists) 'to defend human rights, and keep the Internet free and open' (DDP n.d.).

B. The Sino-Russian cyber security norm preferences

Notwithstanding their nominal agreement with the Five Eyes about existing international law's applicability to cyberspace, China and Russia are not part of the previously mentioned cyberspace norm building initiatives. The Sino-Russian bloc perceives the Budapest Convention, the Tallinn Manual, the GCSC, and the FOC as part of a Western-centric norm building system, infused with the global liberal agenda underpinning and informing the foreign and strategic policies of the Five Eyes. While the Sino-Russian bloc favours new international treaties, rather than the development of non-binding norms, to govern cyberspace, it still participates in developing cyberspace norms mainly through existing multilateral platforms like the UN and the Shanghai Cooperation Organisation (SCO).[7]

Sino-Russian cyberspace norm preferences have three key features. First and foremost is the conceptual difference between 'information security' and 'cyber security'. For the UK (Cabinet Office 2016, 15), cyber security entails 'the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse', while for Australia (DFAT 2017, 23), cyber security enables 'access to online information by individuals, governments and businesses, while ensuring the information and the systems that underpin it are protected from unauthorised access, removal or change'. Hence, for the Five Eyes, cyber security is primarily about the integrity of the systems delivering the information, and only by extension the information itself. By contrast, the Sino-Russian definition of information security entails 'the status of individuals, society and the state and their interests when they are protected from threats, destructive and other negative impacts in the information space' (SCO 2009) and the 'practice of defending the information of individuals, society and the government from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction' (CSIS 2015). Hence, for the Sino-Russian bloc, information security is primarily about the information itself, although the integrity of the systems delivering that information is also crucial. This concept allows governments more arbitrary leeway to interpret what constitutes 'threats, destructive and other negative impacts in the information space'.

[7] The SCO is an intergovernmental organization founded in 2001 by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan (and joined in 2017 by India and Pakistan).

The preference for information security underpins the second central feature of Sino-Russian cyberspace norm preferences, that of cyber sovereignty – a feature consistent with broader Sino-Russian foreign and strategic policy concerns regarding the Five Eyes' global liberal agenda. The SCO's 2009 *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* identified 'information weapons', 'information warfare', and the 'dissemination of information prejudicial to the socio political and socio economic systems, spiritual, moral and cultural environment of other States' as key threats, highlighting 'non-interference' as the key principle of international information security cooperation (Articles 2, 4). In 2016, China's first *National Cyberspace Security Strategy* argued that cyberspace was a new domain 'for national sovereignty', identifying the protection of 'sovereignty in cyberspace' as a key principle (CCM 2016). The Strategy identified 'cyber penetration' and the 'use of networks to interfere in the internal political affairs of other countries' as the foremost 'grave challenge' facing China in cyberspace. It also recognized the growing international 'competition in cyberspace', with its 'strife for the control of strategic resources', as a key cyberspace challenge, taking a swipe at the Five Eyes' dedication to 'cyber deterrence' by warning that 'a small number of countries is strengthening a cyber deterrence strategy, aggravating an arms race in cyberspace, and bringing new challenges to global peace'. 'Resolutely defending sovereignty in cyberspace' was and still is China's primary strategic task.

In April 2015, China and Russia's agreement 'on cooperation in ensuring international information security' formalized the Sino-Russian cyber security bloc. The agreement made clear the bloc's primary concern with cyber sovereignty by emphasizing that 'the state has the sovereign right to define and implement public policies on matters relating to' ICT and the internet (CSIS 2015, 4). Article 2 of the agreement lists the six 'main threats in the field of international information security'. The first, second, fifth, and sixth are all concerned with some form of violating cyber sovereignty; the other two are cyber terrorism and cyber crime. While the agreement's main focus may be on cooperation on internet control to help maintain domestic stability (Segal 2020), Articles 3.3 and 3.13 explicitly discuss 'cooperation in the development and promotion of international law in order to ensure national and international information security' and enhancing 'cooperation and coordination' on 'issues of international information security within the framework of international organizations and fora'.

China and Russia's desire to challenge what they perceive to be the Five Eyes' dominance in shaping how cyberspace is governed is the third key feature of Sino-Russian cyberspace norm preferences. Much like the focus on cyber sovereignty, this feature is underpinned by China and Russia's broader foreign and strategic policies, which seek to reform the post-World War II Five Eyes-dominated global security order to their advantage. China is keen on reforming the Internet's governance, arguing that since cyberspace 'is the common space of activities for mankind', it should be governed following 'a multilateral approach' whereby 'countries, big or small, strong or weak, rich or poor, are all equal members of the international community entitled to equal participation in developing international order and rules in cyberspace' (MFAPRC 2017). China states that the UN 'should play a leading role in coordinating positions of various parties and building international consensus' on the internet's governance, arguing for a 'multilateral' model of internet governance that gives greater control to governments and political regimes. The Sino-Russian internet governance reform agenda is wide, seeking to enhance the UN's role by reforming the Internet Corporation for Assigned Names and Numbers (ICANN) and replacing the Budapest Convention with a new UN cyber crime treaty. China will 'push for institutional reform of the UN Internet Governance Forum to enable it to play a greater role in Internet governance' and 'vigorously promote the reform of ICANN to make it a truly independent international institution, increase its representations and ensure greater openness and transparency in its decision-making and operation' (MFAPRC 2017). Russia views the Budapest Convention's transnationalism as violating 'principles of state sovereignty and non-interference' and has won support at the UN for a 'committee of experts' to consider the development of a new cyber crime treaty to replace it (Segal 2020).

The Sino-Russian bloc has primarily used the UN and SCO to promote its vision of the governance of cyberspace and cyberspace norm preferences. The aforementioned 2009 SCO Agreement made clear the Sino-Russian primary concern with information security and full control of data within a state's territory. Building on this, in September 2011, China, Russia, Tajikistan, and Uzbekistan submitted to the UN General Assembly their proposal for a voluntary *International Code of Conduct for Information Security*. It outlined cyberspace norms which, among other issues, called on states to comply with the UN Charter and respect the 'sovereignty, territorial integrity and political independence' of other states; abstain from using ICT for hostile activities and 'acts of aggression'; prevent states from using their ICT advantages 'to threaten the political, economic and social security of other countries'; promote 'multilateral' governance of the internet; and settle disputes peacefully, refraining from 'the threat or use of force'. In highlighting the primacy of cyber sovereignty, the Code affirmed the rights of states to 'protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage' (UN A/66/359 [2011], 4–5). Finally, in January 2015, the Sino-Russian bloc submitted to the UN General Assembly a revised *International Code of Conduct for Information Security*, which reiterated their focus on cyber sovereignty, reaffirming the rights of states to protect their 'information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage' (UN A/69/723 [2015], 4–6).

4. CONCLUSION

The development of norms of responsible state behaviour in cyberspace is fundamentally a political process, underpinned by values, ideologies, and interests inherent in a state's foreign and strategic policy considerations. States do not seek to neutrally shape norms in cyberspace for the sake of some abstract universal good but rather to expand their own ideological preferences and values and advance their own 'economic and security interests' (Cabinet Office 2016, 9; US 2018, 3). Therefore, cyberspace norm building entails the contestation and competition of ideas, values, and interests inherent in 'regular' international relations – it is the continuation of foreign and strategic policy by other means. All of this is visible in the cyberspace 'Great Game', in which the Five Eyes and the Sino-Russian bloc compete to dominate the governance of cyberspace and global cyberspace norms. Two fundamentally different visions, underpinned by irreconcilable political ideologies, values, and interests promoted by the world's greatest cyber powers, highlight the overwhelming importance and seriousness of this competition.

Both the Five Eyes and the Sino-Russian bloc agree that existing international law applies to cyberspace, but their approaches to the governance of cyberspace exhibit substantive conceptual differences. The Five Eyes' preference for 'cyber security' and the Sino-Russian preference for 'information security' place primary focus on two different issues: securing the infrastructure and processes through which information in cyberspace is accessed versus securing the very information that is being accessed. The Five Eyes' preference for a 'multi-stakeholder' governance of the internet and the Sino-Russian preference for a 'multilateral' approach are also different: the former emphasizes the role of non-governmental actors, staying true to the internet's diffuse origins and operational nature, while the latter emphasizes the primacy of governments and state officials in a more centralized approach. Finally, although the Five Eyes' preference for 'transnationalism' (open internet) and the Sino-Russian preference for 'cyber sovereignty' is not underpinned by a substantive conceptual difference, the significant difference in emphasis placed on this issue has made it arguably the most fundamental point of contention between the two blocs. While both blocs subscribe to the notion of cyber sovereignty, the Five Eyes emphasize the virtues of an open internet and a transnational approach to data management (partially because of their dominance in the development of cyberspace), while the Sino-Russian bloc emphasizes the virtues of territorial integrity and sovereignty (partially because of their weariness of, and desire to challenge, the Five Eyes' dominance in cyberspace).

The implications of the 'Great Game' for the governance of cyberspace are significant. The contested and competitive nature of the 'Great Game' has entrenched 'norm siloing', whereby like-minded states with shared ideologies, values, and interests band together to establish and promote favoured cyberspace norm preferences, 'leading to competing or conflicting islands of normality' (Finnemore and Hollis 2016, 466). However, while such cyberspace norm building may be easier to achieve with like-minded states, those states are usually not the ones whose malicious cyber activity such norms aim to constrain. Moreover, the 'rise of digital authoritarianism' and the decline of global internet freedoms suggests that the Sino-Russian bloc may be slowly gaining the upper hand in the cyberspace 'Great Game' (Shahbaz 2018). The widespread concern for the survival of political regimes with varying degrees of authoritarianism and patrimonialism, coupled with low governmental levels of cyber capability and resources, will make many UN member states fundamentally more sympathetic to the Sino-Russian preference for information security and cyber sovereignty. Although the Five Eyes are powerful enough to maintain their cyber dominance for the foreseeable future, to counter the Sino-Russian bloc they will probably reinvigorate efforts to promote their vision of cyber security and a free and open internet. This will increase the competitiveness and pitfalls of failure in the cyberspace 'Great Game', with neither side likely to 'win', because the appeal of their cyberspace norm preferences will vary depending on the extent to which other states perceive those norms as compatible (or incompatible) with their own ideologies and values, and helpful (or unhelpful) in fulfilling their own wider foreign policy and strategic interests. The cyberspace 'Great Game' will remain a defining feature of global efforts to govern cyberspace in the 2020s, and it is highly unlikely that the latest UNGGE session (2019–2021) will change that in any substantive way.

REFERENCES

Barrinha, Andrew, and Thomas Renard. 2020. 'Power and Diplomacy in the Post-Liberal Cyberspace'. *International Affairs* 96, no. 3: 749–766.

Bolt, Paul J., and Sharyl N. Cross. 2018. *China, Russia, and Twenty-First Century Global Geopolitics*. Oxford: Oxford University Press.

Cabinet Office. 2011. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. https://www.gov.uk/government/publications/cyber-security-strategy.

Cabinet Office. 2016. *National Cyber Security Strategy 2016–2021*. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Center for Strategic and International Studies (CSIS). 2015. *Sino-Russian Cybersecurity Agreement 2015*. https://www.csis.org/blogs/strategic-technologies-blog/sino-russian-cybersecurity-agreement-2015.

China Copyright and Media (CCM). 2016. *National Cyberspace Security Strategy*. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

Clausewitz, Carl von. 2007. *On War*. Oxford: Oxford University Press.

Commonwealth of Australia. 2016. *Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf.

Cooperative Cyber Defence Centre of Excellence (CCDCOE). n.d. *About Us/History*. https://ccdcoe.org/about-us/.

Council of Europe. n.d. *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Cox, James. 2012. 'Canada and the Five Eyes Intelligence Community'. *OpenCanada.Org*. 18 December 2012. https://opencanada.org/canada-and-the-five-eyes-intelligence-community/.

Department of Foreign Affairs and Trade (DFAT). 2017. *Australia's International Cyber Engagement Strategy*. https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/index.html.

Department of Homeland Security (DHS). 2016. *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security*. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Digital Defenders Partnership (DDP). n.d. *About*. https://www.digitaldefenders.org/about/.

Duckett, Chris. 2020. 'Canadian Major Telcos Effectively Lock Huawei out of 5G Build'. ZDNet. 3 June 2020. https://www.zdnet.com/article/canadian-major-telcos-effectively-lock-huawei-out-of-5g-build/.

Finnemore, Martha, and Duncan B. Hollis. 2016. 'Constructing Norms for Global Cybersecurity'. *American Journal of International Law* 110, no. 3: 425–479.

Freedom Online Coalition (FOC). n.d. *Freedom Online Coalition: Factsheet*. https://freedomonlinecoalition.com/about-us/members/.

Global Commission on the Stability of Cyberspace (GCSC). 2019. *Advancing Cyberstability*. The Hague Centre for Strategic Studies and EastWest Institute. https://cyberstability.org/report/.

Global Change Data Lab (GCDL). n.d. 'Share of the Population Using the Internet, 1990 to 2017'. https://ourworldindata.org/grapher/share-of-individuals-using-the-internet?tab=chart&country=AUS~CAN~USA~GBR~NZL.

Gold, Hadas. 2020. 'UK Bans Huawei from its 5G Network in Rapid About-Face'. *CNN*. 14 July 2020. https://edition.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html.

Legrand, Tim. 2019. 'The Past, Present and Future of Anglosphere Security Networks: Constitutive Reduction of a Shared Identity'. In *The Anglosphere: Continuity, Dissonance and Location*, edited by Ben Wellings and Andrew Mycock, 56–76. Oxford: Oxford University Press.

Lilly, Bilyana, and Joe Cheravitch. 2020. 'The Past, Present, and Future of Russia's Cyber Strategy and Forces'. In *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*, edited by T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky, 129–155. NATO: CCDCOE Publications.

Lukin, Alexander. 2018. *China and Russia: The New Rapprochement*. Cambridge: Polity Press.

Ministry of Foreign Affairs of the People's Republic of China (MFAPRC). 2017. *International Strategy of Cooperation on Cyberspace*. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

Moon, Louise, and Chad Bray. 2019. 'Donald Trump's Huawei Ban is a More Severe Threat to Global Economy than Trade War Tariffs, Economists Say'. *South China Morning Post*. 24 May 2019. https://www.scmp.com/business/companies/article/3011676/trumps-huawei-ban-more-severe-threat-global-economy-trade-war.

National Security Agency Central Security Service (NSACSS). n.d. *UKUSA Agreement 1956*. https://www.nsa.gov/News-Features/Declassified-Documents/UKUSA/.

New Zealand Government. 2015. *New Zealand's Cyber Security Strategy 2015 Action Plan*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/nz-cyber-security-action-plan-december-2015.pdf.

New Zealand Law Commission and Ministry of Justice. 2015. *Review of the Search and Surveillance Act 2012*. Report 141. https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC-R141-Review-of-the-Search-and-Surveillance-Act-2012-final_0.pdf.

Packham, Colin. 2019. 'Exclusive: Australia Concluded China Was Behind Hack on Parliament, Political Parties – Sources'. *Reuters*. 16 September 2019. https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF.

Richelson, Jeffrey T. 2016. *The U.S. Intelligence Community*. 7th edition. Boulder: Westview Press.

Segal, Adam. 2017. *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law: Aegis Paper Series No. 1703. https://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty.

Segal, Adam. 2020. 'Peering into the Future of Sino-Russian Cyber Security Cooperation'. *War on the Rocks*. 10 August 2020. https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/.

Seoul Framework for and Commitment to Open and Secure Cyberspace (Seoul Framework). 2013. https://www.un.org/disarmament/wp-content/uploads/2019/10/ENCLOSED-Seoul-Framework-for-and-Commitment-to-an-Open-and-Secure-Cyberspace.pdf.

Shahbaz, Adrian. 2018. 'The Rise of Digital Authoritarianism. Freedom on the Net 2018'. *Freedom House*. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

Shanghai Cooperation Organization (SCO). 2009. *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*. http://eng.sectsco.org/documents/.

Slezak, Michael, and Ariel Bogle. 2018. 'Huawei Banned from 5G Mobile Infrastructure Rollout in Australia'. *ABC New*s. 23 August 2018. https://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438.

Tikk, Eneken, and Mika Kerttunen. 2017. *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. New York: Cyber Policy Institute. https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf.

Tobin, Meaghan. 2019. 'New Zealand Bans Huawei from 5G, China Has Message for New Zealand'. *South China Morning Post*. 17 February 2019. https://www.scmp.com/week-asia/geopolitics/article/2186402/new-zealand-bans-huawei-china-has-message-new-zealand.

Trump, Donald J. 2019. *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. 15 May 2019. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

UN A/Res/65/201 (2010). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations General Assembly.

UN A/66/359 (2011). *Annex to the Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General*. United Nations General Assembly.

UN A/Res/68/98 (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations General Assembly.

UN A/Res/70/174 (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations General Assembly.

UN A/69/723 (2015). *Annex to the Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General*. United Nations General Assembly.

United Nations Institute for Disarmament Research (UNIDIR). 2016. *Report of the International Security Cyber Issues Workshop Series*. https://unidir.org/publication/report-international-security-cyber-issues-workshop-series.

United States (US). 2011. *International Strategy for Cyberspace*. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

United States (US). 2018. *National Cyber Strategy of the United States of America*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach. 2020. *National Cyber Power Index 2020*. China Cyber Policy Initiative: Belfer Center for Science and International Affairs.

Vucetic, Srdjan. 2010. 'Anglobal Governance?' *Cambridge Review of International Affairs* 23, no. 3: 455–474. https://doi.org/10.1080/09557570903535755.

Wellings, Ben, and Andrew Mycock, eds. 2019. *The Anglosphere: Continuity, Dissonance and Location*. Oxford: Oxford University Press.

Whyte, Christopher, and Brian Mazanec. 2019. *Understanding Cyber Warfare: Politics, Policy and Strategy.* New York: Routledge.

World Internet Conference. n.d. http://www.wuzhenwic.org/.

Wright, Jeremy. 2018. *Cyber and International Law in the 21st Century*. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.