Digitally Docile Global Governance: Have We Got any Closer to International Cybersecurity Norms at this year's G7?

JAMES SNOWDEN

The University of Sheffield

Executive Summary

International threats emanating from cyberspace increasingly encroach on every aspect of public life in a cross-cutting fashion. The result is that we are vitally in need of greater international regulation. This policy brief discusses the specious approach to applying international law in cyberspace outlined by the G7 as part of its 'Building a More Peaceful and Secure World' theme at the 44th G7 Summit in Charlevoix, Canada. It argues that this year no real progress has been made on the issue, with the G7 members missing an important opportunity to work towards a global set of cyber norms that are desperately needed.

The Nature of Cyber Threats

Malicious attacks in cyberspace have been growing in salience on the national security agenda of many states in the last decade. Notable recent attacks include: the suspected Russian denial of service attacks on Estonia's 'paperless government' in 2007; the destruction of over 1,000 Iranian centrifuges in 2010 caused by the Stuxnet worm; last year's NotPetya and WannaCry ransomware, demonstrating the far-reaching consequences of cyber threats, causing turmoil on a global scale; as well as an ever-deepening investigation into claims of interference in the 2016 US presidential election.

Cyberspace has been widely caricatured as the 'wild west web', due to a lack of comprehensive regulation. While this is not entirely true, as norms do exist, it is certainly the case within the 'high politics' of peace and security that there are large gaps evident in the

international approach to cybersecurity. Conflicts in cyberspace are no longer confined to the land, sea, or air, but instead constitute a global battleground where effects are both immediate and potentially devastating.

Speaking in March earlier this year, UN Secretary General Antonio Guterres stated: 'It's high time to have a serious discussion about the international legal framework in which cyberwars take place'. The Charlevoix Summit superficially provides solutions in its insistence on the applicability of 'customary international law, the UN Charter and relevant treaties'. But with no underlying substance or structure on how such rules are congruent in cyberspace, these claims ultimately fall flat.

The G7 and the Application of International Law in Cyberspace

Indeed, the severity of the growing threat from cyberspace has been recognised by the countries of the G7. Released earlier this year, the Foreign Ministers' Communiqué, asserts that the 'various dimensions of cyber cut across all our discussions', and stressed 'the applicability of existing international law to cyberspace'. The gravity of the language used in the Communiqué is well warranted. Cyber-attacks are on the rise: there have been 200 state-sponsored attacks by 19 countries since 2005, including 20 in 2016, according to the *Council on Foreign Relations'* Cyber Tracker. Hence, cybersecurity should have been a particularly pressing issue at this year's summit – which stresses the importance of a rules-based international order – and should have grown the prominent position it has held at previous summits.

At the 2016 G7 leaders' summit in Ise-Shima, Japan, its Principles and Actions on Cyber outlined the leaders' desire to 'promote a strategic framework of international cyber stability consisting of the applicability of existing international law to state behaviour in cyberspace'. This

provided a promising starting point, outlining comprehensively that cyberspace is not a lawless domain and recognising that members of the G7 should lead the way in demonstrating how a mechanism of rights and duties should apply in a cyber context.

Furthermore, last year the G7 Declaration on Responsible State Behaviour in Cyberspace called upon states to publicly explain their views on how international law applies to cyberspace in order to 'increase predictability and stability'. Indeed, last month the Attorney General Jeremy Wright outlined the UK's position on the application of international law in cyberspace for the first time. This was the most substantial outlining of how international law applies in cyberspace from a G7 member since US Department of State Legal Advisor Harold Koh's remarks in 2012.

The UK's position treads much the same path as the 2017 G7 Foreign Ministers' Declaration in Lucca. Yet, while it correctly recognises that because cyberspace is international space it therefore must comply with international law, in particular the UN Charter, it leaves a substantial amount of grey area within its application. Among its most problematic elements are its position on interpreting cyber-attacks within the ambiguous 'use of force' stipulation pursuant to Article 2(4) of the Charter and, consequently the 'armed attack' threshold necessary to trigger self-defence, as per Article 51. Fundamentally, these stem from the inherent problems of attributing cyber-attacks given the anonymity, the speed of attack, and the possibility of such an attack being coordinated across a vast array of jurisdictions (as was the case in Estonia). Thus, given the transcendental nature of cyber-threats, it is vital that it is an issue discussed in multilateral, institutionalised fora, and not treated in a unilateral, state-centric or fragmented sense.

However, progress on cybersecurity in Charlevoix seems to have been

'Trumped' by heated debates over tariffs and trade and the US retroactively pulling endorsement, throwing any potential agreement into disarray. Having been essentially side-lined from the final communiqué, the 44th G7 Summit – a forum and platform upon which increased levels of international cooperation can be reached and maintained – represents a missed opportunity to establish the substantial set of international cybersecurity norms that are desperately needed.

A Digital Geneva Convention?

Given the focus on improving the implementation of International Humanitarian law (IHL) at this year's summit, it comes as a surprise that the issue has been largely neglected in a cyber-context. This is especially the case given that the failure of the UN Group of Governmental Experts (UN GGE) last year was underpinned precisely by a disagreement over the application of IHL in cyberspace.

Moreover, despite the G7's commitment to working with the private sector on cybersecurity, there has been no mention of anything even closely resembling the Digital Geneva Convention laid out by President of Microsoft Brad Smith at the RSA conference last year. This ambitious proposal would enshrine the fundamental IHL principles of distinction and proportionality, protecting civilians and companies from nation-state cyber-attacks or full-blown cyber warfare. A Digital Geneva convention would also recognise that the tech sector would be among the first responders to an attack and thus enable a framework for within-sector commitments to provide collective security mechanisms. The proposal has been widely applauded, yet has gained little traction within the international community – evident in its neglect at the G7.

Charlevoix 2018: The Continuation of a Fragmented and Disordered Approach

As things stand, this is fundamentally problematic. The G7's insistence that existing international law applies in cyberspace is essentially a political veneer that neatly fills the legal gap that cyber threats create. There is a severe lack of clarity surrounding exactly how these existing laws apply as part of the 'Building a More Peaceful and Secure World' framework. Not least, this is because the issue is presented through soundbites with no real substance.

For example, the statement 'States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies' is politically satiable, but fundamentally premised on weak legal reasoning and an ignorance of the complexity of cyberspace. Such a statement again makes no real effort to address the underlying issue of attribution. This is true in both a technical sense, as it seems to be simply transposing cyber threats onto the Articles on State Responsibility without modification, and a legal one, as it conflates various standards of attribution that have long caused tension within international case law in cases of kinetic wrongdoing. Ultimately, this leads to an overarching approach that becomes contingent on its superficial and fragmentary understanding of the application of international law to cyberspace.

Indeed, weak international norms engender confused and disordered state policies. This is evident in the US's recent approach to international cybersecurity. Last year, Trump took a positive step forward by signing an executive order design to provide a framework for 'Improving Critical Infrastructure and Cybersecurity'. Yet despite this, the US government remains vividly ignorant to the unique threats that cyber poses. This is evident particularly in new US National Security Advisor John Bolton's forcible removal of Homeland Security Advisor Tom Bossert and his decision to axe the cybersecurity coordinator's position, once current coordinator Rob Joyce leaves.

Like much of his approach to foreign policy, Bolton has been purporting an expressly aggressive agenda for the US in cyberspace; one which can find no footing in international law and seems to fundamentally misunderstand the nature of cyber threats. In February, as part of his 'retaliatory cyber campaign', he stated: 'we need to create structures of deterrence in cyberspace, as we did with nuclear weapons'. However, threats emanating from cyberspace are in no way the same as nuclear weapons as they have much lower barriers to entry, are easier to carry out, and, as discussed above, are significantly harder to attribute. Therefore, Bolton's unilateralist, Cold War paradigmatic view of international relations ultimately renders his approach to cyberspace anachronistic. It is an isolating position that is only likely to be exacerbated by his recent dismissive remarks on G7 summitry.

In a more directly legal sense, this can be highlighted within retired US Admiral James G. Stavridis's position on forcible countermeasures and unilateral mechanisms for punishment. Again, this represents a fundamental misunderstanding of international law as it conflates a use of force approach with customary law on state responsibility – countermeasures that aim to provide punishment, retribution or securing strategic advantage are not permissible under international law. Such confusion can be seen to be both symptomatic of and contributive to the weak position on cybersecurity that the G7 finds itself in, ultimately remaining superficial and therefore, from a practical standpoint, redundant.

What is surprising is that these are well-established problems in applying existing rules to cyberspace, which have largely been set out within the 2013 Tallinn Manual and last year's Tallinn Manual 2.0. There has been no official support for the manuals from any of the G7 countries. Given that a more progressive and informed approach to international cybersecurity at this year's G7 would have been

expected, taking into account such comprehensively thorough research as is set out in the manuals should be emphasised before next year's summit, due to be hosted by France. Indeed, next year's G7 should aim to provide real collective multilateral traction, working in coordination with leading international civil society organisations and private sector industry in order to move towards a set of coherent and substantial international cybersecurity norms.

Conclusion

The G7's stance taken on cybersecurity this year falls short of the ambitious target of applying existing international law to cyberspace, as set out only two years ago in Ise-Shima. After the 44th G7 Summit we are no closer to having a comprehensive or tangible set of norms through which the underregulated realm of cyberspace can be securitised. Indeed, the issue has been almost entirely neglected. Although last month's Foreign Ministers' Communiqué provides more detail, its content is fundamentally superficial and communicated through politically specious soundbites. It has therefore done little to alleviate the confusion stemming from the fragmented cyber-strategies of its members. As an informal international forum, the G7 presents an opportunity to provide a backdrop against which traction can be made towards a desperately needed set of international cyber norms. This year that opportunity has been missed as regulation in cyberspace remains in a disordered and, ultimately, impracticable state.

James Snowden *is an LLM International Law and Global Justice student at the University of Sheffield.*