

July 2017

Sustaining Progress in International Negotiations on Cybersecurity¹

James Andrew Lewis

Establishing Cyber Norms

Concern over the risk of cyber attack led Russia in 1998 to propose at the United Nations a treaty to limit the use of cyber attack and cyber weapons. The Russian proposal drew on the experience of arms control and disarmament, but it found little support and was opposed by the United States. During the same period, there were also various proposals from the academic community for some sort of formal international cybersecurity convention, but many of these proposals were impractical and they too garnered little support.

Agreement on a binding treaty or convention was politically impossible, given the high levels of distrust among major states, but an alternative approach seemed more promising. Research on an approach that used nonbinding norms and confidence-building measures (CBMs), leading eventually to an environment in which formal agreement would be possible, created a credible alternative to a treaty. The norms-based approach drew on the experience in nonproliferation regimes, such as the Missile Technology Control Regime, and on CBM precedents from the Treaty on Conventional Forces in Europe and similar political-military arrangements developed during the Cold War.

These concepts helped to shape the 2010 report of the second UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE).² This report created a negotiating agenda for international cybersecurity in five recommendations using 94 words, calling for further dialogue among states on norms, "to reduce collective risk and protect critical national and international infrastructure"; on CBMs, "including exchanges of national views on the use of ICTs [information and communication technologies] in conflict"; and for the development of capacity-building measures.³

¹ This work was carried out with the support of the Centre for International Governance Innovation (CIGI), Waterloo, ON, Canada, www.cigionline.org. It is reprinted here with permission.

² UN General Assembly, "Item 94 of the provisional agenda: Developments in the field of information and telecommunications in the context of international security," July 30, 2010, www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

³ Ibid., 8.

From the work of the 2010 GGE and subsequent GGEs, several general observations can be derived for consideration in developing next steps for negotiation:

- The scope and degree of agreement among states determines the effectiveness and utility of a norm.
- Meaningful norms will touch on the vital interests of states. One implication of this is that states will be cautious in agreeing to any norm of substance and will consider norms through the lens of self-interest.
- Norms that build on the existing framework of law and practice that guides state behavior in security matters will be most effective, as they will be easier for states to implement.
- Norms discussions do not take place in a vacuum but are shaped and limited by the larger context for international security.
- There is an unavoidable tension between military stability and universal rights. Existing law and practice reflect accommodations between principles and power that define what is acceptable to sovereign states; agreement on cybersecurity will need similar accommodations.
- Fundamental differences in national approaches to cyber attack also create unavoidable tensions.
- The foundation for adherence to norms is the application of power, both “soft” and “hard,” or the threat of the application of power.
- Process is as important as substance in winning agreement.

The GGE Process after 2017

Looking at the GGE process to date, it has been surprisingly successful. Agreement on norms and CBMs achieved in GGEs, in 2013 and 2015, helped to catalyze international interest in cybersecurity. Between them, the two meetings produced 18 principles for responsible state behavior in cyberspace.

In particular, the 2013 GGE identified foundational norms that embedded cybersecurity in the existing framework of international relations and law. These foundational norms are:

- the applicability of the principles of state sovereignty to cyberspace;
- the centrality of international law and the UN Charter for governing state behavior; and
- the need to respect the rights set forth in the Universal Declaration of Human Rights and other international instruments.⁴

⁴ UN General Assembly, “Item 94 of the provisional agenda: Developments in the field of information and

The 2015 GGE, with some difficulty, elaborated and expanded the concepts laid out in 2013.⁵ However, the larger security environment had deteriorated (and continues to deteriorate), revealing tensions and disputes that constrain progress toward further agreement. At the conclusion of the 2015 GGE, many participants asked if the GGE process had reached the end of its useful life, but deciding what should replace it proved to be difficult. In some respects, the rationale for holding another GGE in 2016–2017 was the inability of the international community to identify a different way forward in its discussion of cybersecurity.

A GGE is supposedly composed of independent experts whose task is to provide advice to the UN Secretary General. In the cybersecurity GGE, however, experts represent their countries and are now usually drawn from foreign ministries. The GGE has evolved into a proxy for negotiation between states and is an increasingly unsatisfactory substitute for direct, formal negotiation. The GGE format is limiting, since the report of the experts cannot exceed 7,000 words (including transmittal documents and the list of expert names and titles). GGE meetings are closed, leading to charges that secret negotiations among a small group of states deprive other nations of a chance to see their views reflected in the final text. While the cybersecurity GGE has grown from 15 members, in the first sessions in 2004, to the current 25, there are complaints that this number is too small to be fully representative. There are discussions on expanding significantly the number of participants—an idea with some merit, although it complicates the work and would require a longer negotiating schedule—but expansion does not resolve the fundamental problems of format and proxy negotiations.

Holding another GGE would be a case of *faute de mieux*, postponing the question on whether it is possible to develop a more formal process. There have been suggestions that it might be time to move these discussions to regular diplomatic processes, such as the Conference on Disarmament (CD), or to a body similar to the UN Office for Outer Space Affairs' Committee on the Peaceful Uses of Outer Space, or to create a new and open-ended working group. Either move could have advantages, such as more inclusivity or transparency, but also disadvantages, such as a record of ineffectiveness in reaching agreement—for example, the CD has been unable to agree on any major issue in decades. These proposals raise countervailing concerns that the negotiating process would be captured by those nations that seek to control content and limit freedom of expression.

The impulse for diffusion among UN bodies creates problems for coherence in cybersecurity negotiations. Currently, the UN First Committee (which considers all matters related to disarmament and international security within the scope of the charter) has been able to maintain leadership over cybersecurity, but other UN bodies, such as the International Telecommunication Union, the UN Economic and Social Council, and others, have sought to assert a role in cybersecurity for themselves. Exactly what expertise a standards body or group focused on development brings to international security is unclear, nor would states be willing to let responsibility for the sensitive issues of conflict and survival fall to bodies that lack responsibility and competence for security. That said, a

telecommunications in the context of international security," June 24, 2013, www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf.

⁵ UN General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary General," July 22, 2015, <http://undocs.org/A/70/172>.

proxy negotiation using a GGE lacks the political heft to squelch these unhelpful challenges.

Arms Control, Disarmament, and Sovereignty

A decision to adhere to a norm reflects three related factors: a state's decision on the norm's utility for its own interests, based on the state's assessment of the likelihood that others will observe it; the value the state places on appearance in the international community; and how well the norm comports with the state's own values. The dynamics of fragmentation in the international system limit the scope for global norms development.

A Western approach to cybersecurity norms would emphasize constraints on attack and the use of force, defining malicious behavior as states' use of cyber techniques for force or coercion, and reiterate commitments to human rights and the existing Internet governance structure. The non-Western alternative places emphasis on the political effect of information and the belief that content is used against states to destabilize their regimes. This explains the long-standing Russian assertion that "information is a weapon." The non-Western alternative is accompanied by a desire for a greater recognition of sovereign rights in cyberspace and a greater role for sovereign states in Internet governance. Western and non-Western views, while often diametrically opposed, do not preclude all possibility for agreement. The precedent of arms control shows that even opponents can agree on stabilizing measures.

Norms for sovereignty and the use of force by states in cyberspace offer the most promising field for agreement among disparate and competing groups of countries. These two issues are compelling as they directly affect the survival of the state. Sovereignty and warfare are, in some ways, facets of the same issue: the state's ability to remain as an independent actor. Fears about potential diminution of state independence, combined with concerns over what is perceived to be a new and powerful form of attack, have a destabilizing effect on international relations.

Nations share a concern over the possibility of cyber attacks that could damage their political independence, drawing on the experience of the 2007 actions against Estonia.⁶ They also share concerns over cyber attacks' ability to damage critical infrastructures, as shown by the Stuxnet and Aramco attacks. In these shared concerns, there is ground for agreement. While the nature of offensive cyber operations is poorly understood, it should be possible to build on the progress made by previous GGEs to define general principles for stability and security.

An informal tally of national experts suggests that there are areas where agreement is unlikely—Internet governance and human rights, particularly involving freedom of expression and access to information. Previous GGEs simply took governance off the table as an issue and papered over the difficulties with rights through the frequent invocation of the Universal Declaration of Human Rights and other instruments.

⁶ "Russia accused of unleashing cyberwar to disable Estonia," *Guardian*, May 16, 2017, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

Cyber “terrorism” is also an area where agreement is unlikely. Since there has been no terrorist use of cyber attack and since no terrorist groups possess these capabilities, the discussion of norms on cyber terrorism becomes a debate over online content and of extraterritorial rules to restrict speech. Similarly, some nations would like to extend the Wassenaar Arrangement restrictions on exports of surveillance technologies, but given the difficulties of defining technologies of concern, it will be difficult to achieve meaningful agreement to restrict acquisitions or transfers.

There has been some discussion among Non-Aligned Movement (NAM) member states of making cyberspace a zone for exclusively peaceful use or a weapons-free zone, building on the precedents of nuclear weapons-free zones, but this concept has several problems. First, it is difficult to verify if a nation is complying with the agreement or not. Weapons-free zones are often a commitment among nations who are incapable of violating it. Second, while those who possess nuclear weapons are bound by implicit norms that constrain use, they are unwilling to renounce these weapons. Third, cyber attack, unlike nuclear attack, does not threaten mass destruction. Cyber attack does not match the ability of nuclear weapons to kill tens of millions of people and cause immense destruction in the space of minutes. This disparity between nuclear and cyber undercuts incentives for nations to forswear the use of cyber attack.

In only a few instances have states agreed to ban entirely some form of military activity, usually in cases involving weapons that have the potential for disproportionate suffering and mass effect. In other instances, the use of force is governed by rules to avoid unnecessary harm to noncombatants without forbidding military activities. Nuclear weapons are an anomaly. No treaty bans their use; acquisition is only banned for those nations outside of an initial set of nuclear powers (and this ban has been conspicuously violated several times). Powerful emotions led to the creation of norms on use and acquisition of weapons of mass destruction; the absence of these emotions regarding cyber threats suggests that states will acquire cyber attack capabilities and use them when they believe it is in their interest to do so. This debate—arms control versus disarmament—goes back to the foundation of the United Nations. Badly managed, it can lead to paralysis, but with some skill an agenda can be designed to promote an arms-control approach (that accepts weapons will be built and used and embeds their use in international humanitarian law) in the near term, while not foreclosing disarmament in the long term.

Similarly, debate over the balance between sovereign rights and universal obligations dates back to the United Nations’ creation. Shifts in state attitudes about sovereignty occur slowly, if at all, but there is a discontinuity between Western preferences (especially Western Europe, after the cataclysm of 1939–1945) and non-Western nations, which tend to place a higher value on “traditional” sovereignty. The 1939–1945 experience leads Europe and other Western states to assign a higher potential risk to sovereignty than is the case elsewhere. Russia, which suffered as much as any other country in World War II, opposes the Western view of limited sovereignty as it is motivated by revanchism and a belief that the Western system is hostile to Russian interests. Russia’s strong desire to reassert traditional sovereignty finds support in many non-Western nations.

Dispute over sovereignty and universal rights has implications for both the substance of norms and the chances of agreement. There is a fundamental divide in current international relations, between those states who argue for universal values and those who believe that universal values are really “Western,” and the derogation of sovereignty that began with the Charter of the United Nations⁷ has gone too far. These nations would prefer to reassert a more traditional view of sovereignty in the relationship between the state and its citizens, one less accommodating of universal values and, as a consequence, in its relations with other states.

Such disagreements are not necessarily fatal to agreement. The most salient example is the UN charter itself, which in Article 2.4 forbids member states from using force against another state, without the approval of the Security Council, and in Article 51, recognizes their inherent right to use force for self-defense without Security Council approval. Underneath this apparent dissonance in the charter is a more complicated discussion of aggression versus defense, but the occasional ambiguity in an agreed text is essential for successful diplomatic negotiation.

Next Steps for Negotiations

Differing national views on the use of force, control of content, governance, and international crime shape the space for agreement on cybersecurity norms and create the landscape for negotiation. There is no consensus among nations on these topics, which creates a challenging environment for continued, meaningful progress on cybersecurity norms. However, parsing different substantive aspects of the GGE’s work, combined with developing a less ad hoc negotiating process, suggest a path forward.

A broad agenda for cybersecurity negotiations that attempts to address the full range of issues, including crime, intellectual property protection, espionage, and military action, may have seemed appropriate in the early days of negotiating but is now impractical. A mature negotiating process would have a different structure than the GGE, with baskets of issues, working groups, and a plenary body. This approach would require a greater investment of time and resources than countries, despite the salience of the cybersecurity issue, are prepared to make. If we discount the constant iteration of banal generalities, cybersecurity norms remain a tertiary issue for the international community.

The disjointed nature of the global discussion reflects a larger problem with the term “cybersecurity,” which means different things to different communities, who define the problem and any solution in varying ways (usually through the prism of their own experience and expertise), and often assert that they naturally should lead. Dissonance can be reduced by defining the objective of international negotiation: to reach agreement on state responsibilities for peace and security in cyberspace, including states’ responsibility for the actions of their citizens, companies, or others subject to their laws, and a commitment to ensure that actions in cyberspace do not contravene their international commitments.

The nexus for negotiation lies at the intersection of political rights, sovereignty, and use of force, and the primary purpose for cybersecurity norms is to limit the risk of conflict. Norms can also be used to

⁷ United Nations, Charter of the United Nations, October 24, 1945, <http://www.un.org/en/charter-united-nations/>.

reaffirm commitments to a free and open Internet, but these issues are contentious and perhaps tertiary, and if it is possible to reach agreement on measures to improve security and stability using commitment from states to renounce certain behaviors without compromising fundamental freedoms, this may be the best outcome now possible. A formal approach to negotiation focused on security would not address all issues or assuage all communities, but it would be the approach most likely to succeed in reducing risk.

James Andrew Lewis is a senior vice president at the Center for Strategic and International Studies in Washington, D.C.

This report is reprinted by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2017 by the Centre for International Governance Innovation. All rights reserved.