CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

TECHNOLOGY POLICY PROGRAM

August 2018

State Practice and Precedent in Cybersecurity Negotiations

James Andrew Lewis

A number of proposals for international cybersecurity negotiations share a common feature: they offer unworkable ideas. The reason for this is the discrepancy between theory and practice, particularly when proposals diverge from state practice, which we can define as how states will behave to maintain or advance their interests. Some proposals also seem to ignore a changed international environment, where the post-1945 ideals, institutions, and powers are in decline and the United States lacks the influence it once had. Proposals that run counter to state practice or that discount the weakening of Western influence face serious and perhaps insurmountable obstacles.

State practice is the touchstone for assessing the viability and utility of a negotiating proposal. Proposals that undercut or harm state interests will not be adopted. The most salient distinction in state practice is between small states, who, lacking power, promote norms and the rule of law to constrain state power, and large states, who generally abide by such constraints as long as it does not interfere with their interests. Thucydides' phrase "the strong do what they can, and the weak suffer what they must" remains as useful a guide to international relations as when it was coined.

An example of how state practice shapes the space for agreement are proposals that states should forswear interference in financial networks. While these ideas have merit, some major powers have been reluctant to endorse them. Being able to follow money transfers and discover illicit accounts is crucial for nonproliferation, counterterrorism, and for determining the size of various dictators and oligarchs' financial holdings. Most financial institutions cooperate with legitimate requests related to crime and law enforcement, but some, as we have seen in the Panama Papers, do not. A new norm would have to be very carefully crafted to allow continued espionage, else larger powers will ignore it. In the worst case, a norm would constrain the United States and its allies without affecting the operations of our opponents, a luxury that we can no longer afford.

The utility of various negotiating proposals is also affected by the decline in U.S. influence, something that began more than a decade ago, and the growth of nationalism, which is in

good measure a reaction to a Pax Americana world and U.S.-led globalization that emerged after 1990. It turns out that we are not one world after all. The millennial vision that the end of the Cold War heralded the arrival of world that would look largely like the United States, where borders were erased by technology and governments replaced by some mix of unelected stakeholders is an artifact, no longer valid, and diplomatic strategies based on it court failure.

The United States is seized by a powerful ideology that devalues government. This applies across the political spectrum—the Obama administration's deference to Silicon Valley was an example of this. Corporations are as powerful as states only in a world where states agree not to use force, and this is not the world today. The use of force may not always take conventional forms, since coercive international acts increasingly rely on cyber operations, but force and coercion by states are displacing the rule of law.

So it is puzzling to announce that "the proposals that are best suited to help shape global governance have come from corporations and civil society groups, not states."[1] States remain the most powerful actors, and large states not afflicted by the U.S. ailment of "disgovernance" do not hesitate to use that power. There is no evidence that China or Russia have much interest in the wishes of corporations and civil society, and they are likely to ignore proposals from such sources.

We also cannot assume that other newly powerful states, such as India, Turkey, or Brazil, will automatically defer to Western business interests or civil society. While Russia and China struggle to make the BRICS a useful alternative to Western institutions, the leaders of India, Brazil, and South Africa show up to BRICS meetings and accord them significance. They share in varying degrees Russian and Chinese concerns over "universal" values. China and Russia argue that these values are inappropriate for non-Western societies. Much of this is driven by the desire of the regimes governing those countries to shield themselves from criticism, but other nations share a discontent with the existing international order.

International security is an issue that states reserve to themselves. States bear primary responsibility for international security and stability because they are the legitimate agents for the use of force, the ultimate source of international power. The multistakeholder model, the basis of internet governance, is inadequate for international security because other stakeholders lack the power and tools necessary for security. If some states choose not to exercise power, it does not invalidate this assertion, but it does create a complicated negotiating environment where the United States and its allies may be at a disadvantage.

When China's Xi Jinping talks of reforming the global governance system, he is not looking to NGOs or corporations for ideas. He has been clear on this point, saying "countries and intergovernmental organizations should shoulder the main responsibilities of security governance, while non-governmental organizations, multinationals, and civil society are

[1] "Private-Sector Initiatives for Cyber Norms: A Summary," Lawfare, June, 2018, https://www.lawfareblog.com/private-sector-initiatives-cyber-norms-summary

encouraged to jointly work for it."[2] Vladimir Putin said something similar at Russia's first International Cybersecurity Congress this month: "it is the job of the state to neutralise (sic) them [cyber threats] and provide cybersecurity in general."[3]

The Proliferation Security Initiative (PSI) and Cybersecurity

If there is a theme in the current U.S. approach to international cybersecurity, it is that there will be no improvement until there are consequences for malicious actions in cyberspace. This reflects a recognition of the improbability of the United States and its opponents agreeing to much more than was agreed to in the UN in 2015. The space for agreement with adversaries has shrunk. Agreement on norms unaccompanied by consequences for misbehavior has not reshaped our opponents' perception of risk in undertaking malicious cyber actions.

In 2017, the administration adopted a strategy of gaining agreement among likeminded nations to cooperate, on an ad hoc basis, in imposing consequences on nations that flout the 2015 UN Group of Government Experts norms that were endorsed by Un Member states. "Like-minded" nations (which usually means Western democracies) are moving towards a consensus that some kind of framework for collaboration and collective response is essential for better cybersecurity, but turning this shared desire into action will be difficult. The United States chose to pursue a series of bilateral agreements with close security partners rather than attempt to build a multilateral approach (although this was not ruled out as a later development). Some have proposed (again) that one model for this approach could be based on the Proliferation Security Initiative (PSI), a successful effort to interdict illicit shipments of material related to weapons of mass destruction. [4]

PSI has attractive features. It is voluntary and effective, but part of the reason for its effectiveness is that nonproliferation rests on a broad set of well-established norms, binding treaties, and national laws. This makes it very different from cybersecurity, where norms are new and still contentious, and there is no treaty of any kind. When the idea of a PSI-like approach to international cooperation in cybersecurity was first raised by the United States with its allies in 2009, it met with a mixed reception. The reasons for this have not changed in the intervening years, and the environment for cooperative action with allies has become, if anything, less favorable.

Proliferation usually involves tangible objects. Missile parts are hidden on a freighter; navies and customs services can interdict and search the ship. If the proscribed object is found, there is little doubt of a violation and few countries object to the search. Cybersecurity does not involve tangible objects, and a search will likely raise sovereignty problems not found on

[2] http://english.scio.gov.cn/topnews/2017-09/27/content_41653323.htm
[3] Publication date: July 6, 2018, http://en.kremlin.ru/events/president/news/57957
[4] "A Proliferation Security Initiative for Cyber Cooperation?" Lawfare, June 2018, https://www.lawfareblog.com/proliferation-security-initiative-cyber-cooperation

the high seas, making enforcement more difficult. It is one thing to accuse Iran or North Korea of WMD violations, another to take on China or Russia over cyber actions.

Many PSI seizures are based on intelligence, when the United States or another security partner will tip off the country best placed to intervene. When you search a ship and find WMD technology, there is no need to tell how you knew it was there. The political risk of interdiction of vessel (often sailing under a third-country flag of convenience) in a port or on the high seas is much lower than taking action against a large and hostile power on its home networks. The understandings among states about the applicability of sovereignty are much less clear in cyberspace than in the physical world.

The intelligence behind a cyber "interdiction" may be unambiguous to the nation that collected it, but not to other countries, since the collector (often the United States or United Kingdom) may be unwilling to share sources and methods. This would put partners in the position of acting in a politically charged environment on the basis of trust. One European cyber official said that their government (a NATO ally) would be hard-pressed to act against a major power like Russia for a cyber incident without very compelling evidence that it could make public, to explain to its legislators and population why it was acting. Conversations with other European cyber officials point to attribution, trust, and agreement on appropriate consequences as the most difficult problem for a multilateral approach to imposing consequences on bad actors. This was true even before the current disputes between Europe and the United States further frayed trust and a willingness to cooperate.

No IAEA for Cyberspace

Trustworthy and releasable evidence on attribution of the source of a cyberattack is crucial for an international (or like-minded) response. One proposed solution to the attribution and trust problem is to create a new international organization, private or governmental, for attribution of the sources of a cyberattack. Recurrent calls for a new institution, perhaps something like the International Atomic Energy Agency (IAEA), to investigate cyberattacks and identify their source discount major problems that any such organization would face. The desire to have an impartial body of experts examine cyberattacks and determine who is responsible is understandable, but these proposals underestimate the difficulty of creating such a process absent the lack of formal agreement among states while also overvaluing the benefits of an attribution process where the chief investigators may also be the target of the investigation.

The IAEA works because it is based on treaty commitments and is linked to the UN Security Council for enforcement. The IAEA is part of the UN institutional structure. It grew out of a 1953 Presidential proposal by the United States to the UN General Assembly. Three years later, a group of 12 countries began negotiating the IAEA's statute, which came into force in

1957.[5] The statute laid out the IAEA's mission, funding, and the relationship with the UN (and the new agency's degree of autonomy from the UN and UN processes was a point of contention in the 12-nation group).

The IAEA derives its authority from the Treaty on the Nonproliferation of Nuclear Weapons (NPT). After a ten-year negotiating process, nuclear weapons states committed to ultimately give up nuclear weapons in exchange for a commitment by nonnuclear weapon states not to develop or acquire nuclear weapons. The NPT gives the IAEA the mission and authority to investigate and verify compliance with the treaty. The IAEA itself cannot impose sanctions, but it can report to the Security Council when a nation is failing to comply with its NPT commitments; the Security Council can then decide if sanctions should be imposed.

Nuclear weapons states also agreed not to transfer weapons technology. The nonnuclear weapons states sign safeguard agreements with the IAEA that gives the agency the authority to inspect and verify that a nonnuclear weapon state is complying with its NPT obligations. The IAEA does not inspect nuclear weapons states for verification, making it an imperfect model for investigation of cyberattack, since it is difficult to see under what circumstances states with cyberattack capabilities would be willing to inspect themselves or cooperate in an investigation into an incident in which they were involved.

Simply assembling cyber experts in some new attribution organization is not enough. The difficulties of attribution in cyberspace are more political than technical. The IAEA's effectiveness is derived not only from its institutional expertise but from its relation to the NPT and to the Security Council. Politically, it is in the interest of nuclear weapons states to prevent nuclear proliferation. This usually ensures their support. The absence of a cyber treaty and the commitments that would underpin it makes an IAEA-like approach to cyberattack impractical. An inspection agency that lacked some organic linkage to the UN Security Council and its ability to impose sanctions would be ineffective from the start. Great powers are not deterred by "naming and shaming," and states would simply ignore, dispute, or reject a cyber inspection agency's findings.

The NPT provides an essential element of legitimacy and consent for IAEA activities. Absent a similar treaty on cyber activities, a new cyber verification entity would lack authority and legitimacy. As an aside, it is hard to see the nations of the world agreeing that those who now possess cyberattack capabilities (perhaps 20 countries) should be allowed to keep them while the other 170 nations renounce the acquisition of offensive capabilities. Nor is the development or acquisition of cyberattack capabilities easy to control. It is not easy to define offensive capabilities or distinguish them from legitimate research activities, as the experience of the Wassenaar Arrangement has demonstrated. The nuclear industry is relatively small when compared to the software industry, with a less important role in national economies and a much smaller number of companies. This difference in scope

[5] The five permanent members of the UN Security Council and seven regionally representative countries. David Fischer, "History of the International Atomic Energy Agency: The First Forty Years," http://www-pub.iaea.org/MTCD/publications/PDF/Pub1032_web.pdf

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199

creates significant problems for verification and control.

The NPT is not a good model for cybersecurity. In only a few instances have states agreed to ban entirely some form of military activity, and then only in cases involving weapons that cause disproportionate suffering or mass effect. In other instances, the use of force is governed by rules to avoid unnecessary harm to noncombatants. 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). While those who possess nuclear weapons are bound by implicit norms that constrain use, they are unwilling to renounce these weapons.

Most importantly, cyberattack, unlike nuclear weapons, does not threaten mass destruction—cyberattack does not match the ability of nuclear weapons to kill tens of millions of people and cause vast destruction in the space of minutes.[6] The absence of the powerful fears and emotions that led to the creation of norms for weapons of mass destruction means that states will not be dissuaded from acquiring cyberattack capabilities and use them when they believe it is in their interest to do so.

Given the ease of acquisition, the close linkage of military cyber operations to espionage and electronic warfare (and no state is going to renounce these), and the difficulties of verification, we are not going to be able to obtain an NPT for cyberspace. A treaty renouncing cyber "weapons' is unlikely, and absent such a global commitment, an IAEA-like institution would face insurmountable political obstacles.

This caveat also applies to using the Organization for the Prohibition of Chemical Weapons (OPCW), as a model. OPCW governs technologies that include chemicals with widespread commercial use, something that makes it more like cyber activities than PSI or IAEA. The OPCW implements the Chemical Weapons Convention (CWC), which was negotiated in the Conference on Disarmament, a Geneva-based body that is part of the UN system. The timeline of the OPCW is in itself a useful precedent for cybersecurity—it took 12 years to negotiate the treaty, and another 4 years for the treaty enter into force. The CWC was built on a 1925 convention prohibiting the use of chemical weapons, and experience and support of a group of likeminded states (the Australia Group) established in 1985. OPCW allows for intrusive "challenge" inspections for verifying commitments to ban chemical weapons, but given the closeness of cyber operations to sensitive national security activities, like espionage, it is difficult to see how any kind of challenge inspection would ever win agreement.

If the desired outcome is some kind of cybersecurity regime similar to IAEA or OPCW, it will need to be based on formal agreement, take years to negotiate, and require continued high-level political support. All of this has so far been lacking for cybersecurity. The terrain for international cooperation on cybersecurity is marked by ambiguous evidence, a conflictive

[6] This disparity between nuclear and cyber also suggests the need for a closer examination of the discussion of "strategic stability," another inheritance from the nuclear age.

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199

environment, an absence of agreement, and the lack of an existential threat. This means we should not expect to transplant ideas easily from nonproliferation or arms control into cybersecurity.

Uncharted Terrain Requires New Concepts

The discussion of cybersecurity reflects weaknesses in the field. It suffers from ahistoricism —there are only a few compelling histories of cybersecurity[7]—and there can be an overreliance on inductive methods and analogy (objections that might also apply generally to the study of international relations[8]). Analogy must be used carefully in situations where dissimilarities are as great as the likenesses, and an ample literature has discussed the disadvantages of nuclear analogies and precedents for cybersecurity. There is also growing appreciation that the nature of interstate conflict has changed in ways that affect the discussion of norms and negotiations, as opponents choose strategies designed to stay below the use of force threshold and evade the strictures of existing international law. This means a discussion of precedents such as IAEA's, PSI's, Solariums, and even concepts like Strategic Stability or norms should be approached with caution.

Meaningful agreement on cybersecurity will affect states' vital interests. One implication of this is that states will be cautious in agreeing to anything and will consider agreement through the lens of self-interest. States may be particularly careful in approaching cybersecurity, given the opaqueness of risk and the disparity in knowledge of cyber issues, and cyber's significant connections to human rights, national security, and economic growth. Cyber capabilities have introduced a new dynamic into international relations whose effects states have yet to fully calculate. In these circumstances, it can be difficult to calculate where a state's national interests lie.

In the near term, agreements that build on the prevailing framework of law and practice that guides state behavior will be the most compelling. Agreement by a state is an abrogation of its rights and privileges as a sovereign; the state is in essence surrendering some freedom of action. The landscape for this diminution of sovereignty is complex. Over the last century, states have collectively acceded to numerous limitations on their powers over trade, security, and internal political rights, but these agreements were usually reached after long and arduous negotiations, often through an incremental process and sometimes driven by crisis. We should expect the same complexities for cybersecurity.

There has been some progress, with an endorsement of general norms, the most important of which embed cyberattack in the existing framework of international law. There has been agreement on initial confidence building measures in the Organization for Security Cooperation in Europe, the ASEAN Regional Forum, and the Organization of American States. The UN is entering its eighth year of negotiations (now buttressed by the efforts of the

[7] Jason Healy's *A Fierce Domain: Cyber Conflict, 1986 to 2012*. May be the best history available.
[8] By scholars such as John Lewis Gaddis

Secretary General). But the progress of international negotiations on cybersecurity remains slow, outpaced by the development of offensive techniques and their use, since there is no existential threat that would drive the major powers to make the concessions needed for progress in cybersecurity. Further progress will require painstaking effort that takes into account state practice and an international political dynamic that erodes support for Western norms; as one leading Chinese scholar put it, "We are moving away from a state in which international norms are led by Western liberalism to a state where international norms are no longer respected."[9]

Cyber negotiations are shaped by the larger political environment for international relations. Existing institutions and relationships are under duress, and the framework of relations among states is evolving to accommodate both rising powers and assertive antidemocratic states. This is not necessarily the decline of the West, but it is clear that Western values, shaped by democracy, human rights, and open markets, are on the defensive. The environment for agreement on cybersecurity (or other issues) will be contentious and marked by suspicion.

What does this mean for negotiation? It means collaboration will be more difficult—with opponents and, unfortunately, with allies. Any agreement or institution will need to emerge from the interaction among states with different and competing interests—this is not 1945 when there was widespread consensus on the need for stabilizing institutions, nor is it 1975, when competing powers were ready to reach accommodation. The absence of an agreed international framework for cybersecurity, accompanied by increased international tensions, and challenges to transatlantic leadership, limit the ability to reach agreement along the lines of PSI or IAEA.

There are three areas where international agreement could be usefully pursued: to control and constrain the use of cyberattack, or ban some categories of attacks entirely; to endorse existing commitments to human rights in their extension into cyberspace; and to endorse the multistakeholder model of internet governance, perhaps reformed to accommodate non-western states. Of these, the first is the area where the interests of opposing states are most likely to overlap.

This does not mean there is no space for negotiation. The immediate focus should be on assembling likeminded nations to operationalize norms and consequences, while continuing to explore whether further agreement with opponents is possible at the margins of what was agreed in 2015. Progress requires finding some way to involve private actors. It also requires recognition of the central role of the UN. While many Americans discount the UN, other countries see it as the locus of international governance and a U.S. strategy must take this into account. Precedents from other domains are of limited value for cybersecurity. We need ideas that recognize the world as it is, conflictive and dominated by states, and not as we imagined it when the United States was unchallenged.

[9] http://chinamediaproject.org/2018/06/26/yan-xuetong-on-the-bipolar-state-of-our-world/.

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