Private Actors' Roles in International Cybersecurity Agreements – Unlearned Lessons

Dr. James Lewis

Vocal communities in the West demand a role in international public policy for cyberspace. In some areas of activity, such as privacy, controls on social media content, commercial issues like anti-trust or digital taxation, this private sector involvement is essential. But the unlearned lesson is that it is equally important for national security, as is the effective negotiation on security, which is still the purview of states.

One reason for these demands is the erosion of the clear division between internet security and internet governance. Internet governance has been the domain of a multistakeholder community. The members of the multistakeholders community increasingly expect to play a similar role in questions of international cybersecurity. Conversely, most governments had been content to leave internet governance to civil society and corporations, but now, as governance affects their economies and safety, some want a more prominent or even guiding role in the digital world. This confluence - it could even be described as a collision - over roles and responsibilities is complicated by China and Russia's differing visions for security, data governance, and sovereignty. The tensions between multistakeholders and government and between democracy and authoritarian views of digital governance complicate the discussions of the role of the private sector.

To draw upon precedent, in 1915, when it became clear that World War One would not end anytime soon, a wealthy American business leader, Henry Ford, launched a peace initiative. He bought a ship, filled it with pacifists, ministers, and academics (creating the ancestor of the multistakeholder community), and set sail for Europe to persuade the combatants to embrace peace. The warring powers did not warmly receive Ford's well-intentioned effort. At best, they considered him naive. Media coverage in the US was

James Lewis is a Senior Vice President at CSIS and has authored numerous publications while at CSIS on cybersecurity and how technology is reshaping politics, economies, and security. Before joining CSIS, he worked as a diplomat and a member of the Senior Executive Service. Lewis was the Rapporteur for the UN's 2010, 2013, and 2015 Group of Government Experts on Information Security. He is frequently quoted in the media, has testified numerous times before Congress, and received his Ph.D. from the University of Chicago.

critical, sarcastic, and openly hostile in London, Paris, and Berlin. The fate of the well-intentioned Peace Ship is a precedent for proposals to create Cyber Peace or a Digital Geneva Convention.

It is not a perfect precedent, however, because of political changes since 1915. One difference is a perception in democratic societies that cyberspace is too important to be entrusted solely to states, but the more important change is how states use coercion in cyberspace. Cyberconflict is a central battle zone in the new conflict between democracies and authoritarians, and certainly, the authoritarians have no intention of forsaking this battle.

It's worth noting that having non-governmental actors renounce cyberwar and cyber "weapons" is like having vegetarians agree to renounce meat consumption. Today's great powers find themselves in a growing conflict over global governance—essentially between a democratic model that endorses the rule of law and an authoritarian alternative driven by power, regime survival, and not rules. In this contest, democratic states should not renounce cyber weapons and their use unless they are suicidal. States must defend themselves and their citizens. If they fail in this central responsibility, their place will ultimately be taken not by some amorphous group of civil society actors or corporations but by another set of leaders or, in the worst case, another, more aggressive State.

The argument for private sector role cannot be based on the assertion that since the private sector owns and operates 80 or 90 percent of the networks, it bears special responsibility. This dubious statistic is immaterial to the use of force and originally came from lobbyists who argued against internet regulation. In 1914, the private sector owned 80 or 90 percent of the ships afloat but did argue for a role in naval warfare. A few private vessels were armed and made combatants, but they invariably lost any engagement with a proper warship, a

precedent that advocates for private hack-back may wish to consider as they engage the FSB, PLA, or IRGC. Nor were private ship owners invited to the post-War conferences held to reach an agreement to reduce naval armaments and end ship-building arms races. Some argue that since companies operate the networks over which attacks are transmitted, their voices should be heard. Their voices should be heard but in a supporting role. The lesson here is that being a victim does not justify or guarantee a seat at the negotiating table. Entree is provided only based on the cards one brings to the game, and for great power competition, this requires more than cyber-attack capabilities.

Today's tech giants have an array of software tools and could build and use offensive weapons if they chose to violate the law. This leads some to argue that they deserve a seat at the negotiating table since they could engage in conflict. The same could be argued for Russian organized crime, but the Russian state would not permit this. In any case, there is a ceiling on the private potential for offense since companies lack the full scope of military and intelligence assets and are more vulnerable to coercion, particularly from China.

An equally important limitation is the status of private actors under international law, which would make retaliatory action by them a crime, not self-defense. While the authority of states has been diluted in many areas, this is not the case for the use of force and possession of the capability for organized violence at scale, where states still have a monopoly.

Increasing Conflict Constrains Negotiations

The role of the private sector is also shaped by increased inter-state conflict. The international environment is increasingly unstable, and the direction of international affairs is towards greater conflict. It is no longer safe to discount the possibility of armed conflict between major powers, even if these conflicts might be limited in duration and scope. The increased level of international dispute means that cyberspace is a contested domain, where opponents maneuver to position themselves for advantage now and in the event of a conflict.

The absence of overt, formal conflict and the interconnections created by globalization makes it easy to ignore how the international environment has changed. Nations are already in deep conflict, even if it is not the kind of wars declared in 1914 or 1939. Today's conflicts usually involve non-military modes of competition (at least so far). The laws of war were designed for the last century and are difficult to apply to current conflict, chiefly in that the old distinction between espionage and warfare no longer makes sense. The reluctance to admit that nations are in an unavoidable fight is not unusual for democracies. When Ford set sail for Europe or the students at Oxford University declared in 1933, they would never fight a war. Unfortunately, in both cases, authoritarian opponents were not similarly dissuaded.

That said, the future of war, at least among major powers, will try to avoid direct conventional conflict. Wars between big, heavily armed states are expensive and risky, particularly if they involve nuclear weapons. Big countries will not renounce war—Russia, the US, and China

frequently use force or the threat of force—but they will try to avoid open warfare with each other. Opponents will exploit the grey areas in international law and practice inflicting damage without triggering armed conflict. If big countries do stumble into war, cyber-attacks will be a part of the fighting, but cyber operations are not waiting for the outbreak of armed conflict. Cyber operations are a new way to exercise national power without stumbling into conventional conflict. They are ideal for the new strategic environment. How countries will use cyber operations is determined by their larger interests, their risk tolerance, and by their existing strategies, experience, and institutions.

Changes in how nations use force or its alternatives complicate the agenda for negotiation because demarcations between peace and war, or civilian and combatant, are no longer clear. One reason for an increased civil society and private sector role is that the Internet has reshaped public expectations for openness and transparency in democracies. This blurring contributes to the question of who speaks appropriately for the actors in a cyber conflict. For democracies, the use of cyber operations is shaped by public perceptions (among citizens, civil society, and other private actors) of the rationale for action, particularly coercive action. Private sector and civil society involvement have become essential for legitimacy, making cyber negotiation no longer solely the domain of states. It would be unthinkable for western nations not to involve the private sector somehow, which does unavoidably complicate the task of western negotiators.

However, the underlying lesson is that actions needed to gain domestic political support do not guarantee international effect. Agreements that lack commitments from the most powerful states or fly in the face of strategic necessity are of limited value, even if private sector actors support them. The 1907 Hague Convention included a prohibition against bombarding undefended civilian targets and was amended in the 1920s (Article XXIV) to similarly restrict the use of aerial bombardment. Another unfortunate precedent is the Kellogg-Briand Pact of 1929, where states agreed not to engage in war (also signed in Paris). At the start of the Second World War, President Roosevelt appealed to belligerents on September 1, 1939, to only use air attacks against military targets and observe their Hague Convention commitments not to attack civilian populations in undefended cities. Britain, France, and Germany quickly agreed to this, but their commitments collapsed (immediately for authoritarian Germany) in the face of military necessity.

Similarly, civil society recently led a successful effort to draft a UN Convention banning nuclear weapons, but no nuclear power has signed it, and the behavior of the nuclear state is unaffected. These examples suggest that while symbolic agreements may serve useful political purposes within the western community, they are inadequate at constraining the use of force. It is telling that the Paris Accord was unable to attract support from members of the authoritarian group of states, suggesting a profound disinterest in a multistakeholder approach to cybersecurity negotiations.

Most cyber incidents fall into the categories of crime and violations of national sovereignty. They are not an "act of war" (a rhetorical term rather than a legal threshold) and do not involve the use of force as it is traditionally defined. The most damaging cyber incidents are actions by states as part of some larger interstate conflict. We will only see physical destruction and casualties from cyber operations when they are part of some larger armed conflict. Such conflicts will involve a combination of weapons—cyber actions will be only one tool. The low-level cyber actions that we have seen to date have a corrosive effect and can be destabilizing, but we do not want to mistake them for warfare and its high level of violence and destruction (a measurable difference). This is important because, in the absence of the risk of significant damage that armed conflict brings, there is little incentive for states with offensive cyber capabilities to make concessions in their use, much less agree to disarm.

The Value of Norms

Powerful states will not any time soon accept a "Cyber Geneva Convention," the binding convention governing cyber conflict sought by private actors. The groundwork of common understandings has not been laid, and these common understandings usually grow from a shared experience of a conflict that both sides wish to avoid repeating. Both the Geneva Convention (and its protocols) and the Hague Convention that preceded it followed violent wars. These agreements were reactive, driven by the experience of warfare. But, despite the standard exaggeration of the risk and effect of cyber-attack, there has been no cyberwar: no deaths, no causalities, minimal destruction. The serious moral imperative which is created by violence and can lead to agreement on restraint is lacking. Those who wield the most power in cyberspace when it comes to offensive action are not ready to agree to stop. This means that the efforts to create cyber peace are, at best, a rehearsal for negotiation and, at worst, a distraction.

Global agreement in 2021 on a framework of responsible state behavior was a significant step forward for building international cybersecurity in a stable, rules-based environment. Still, experience has shown that agreement on norms by itself is not enough to achieve the desired outcome. While there has been a debate over the usefulness of creating a framework of rules for cyber conflict if all do not observe them, most scholars and western government practitioners agree that these frameworks are still worthwhile for cyber conflict. Their usefulness arises not only because a framework of rules exists and some combatant powers have agreed to observe them, but it is also that they provide a justification for counteraction against those who do not observe them. This may be the most important contribution of norms at this time. For norms to have an effect, there must be consequences for nations who choose not to observe them.

Consequences mean the range of internationally lawful responses available to states who are the victim or target of malicious actions that run counter to agreed norms. While there has been some progress towards the imposition of consequences (such as sanctions by the EU

or indictments by the US), this has been an ad hoc and disjointed process. Even like-minded nations have yet to develop common views on the full range of internationally lawful responses to malicious actions that run counter to agreed norms, on how to anchor them in a rules-based approach to international order, and on how to harness broader global support.

The successful conclusion of the United Nations Open-Ended Working Group (OEWG) opened many avenues for future work in international cooperation in cybersecurity. One of the most important is that the OEWG reinforced the global applicability of existing international law and the norms developed by the 2015 UN Group of Government Experts (GGE), which, together with confidence-building measures and capacity building, consolidated an initial framework for responsible state behavior in cyberspace. This success highlights the question of how states observe 2015 norms. Some of this involves capacity building so that states have the ability to implement norms in their national policies and actions, but it primarily entails a discussion of what the consequences should be when norms are not observed.

This is not a new issue. In September 2019, 28 like-minded nations issued a Joint Statement at the UN on advancing responsible state behavior in cyberspace. These countries agreed to "work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law." Norms and international law are essential to this discussion of consequences. Ultimately, the agreed norms can reinforce international law to reduce cyber conflict. In the interim, however, it would be useful to consider both a menu of voluntary actions to hold states accountable and the issues that accountability unavoidably raises. These include evidentiary standards, attribution, and information-sharing; mechanisms for coordination of collective action; the relation to other measures, such as the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (or so-called EU Cyber Diplomacy Toolbox); harmonization with international law and the implications of other treaty obligations for collective self-defense.

The status of international negotiations on cybersecurity remains slow, far outpaced by the development of offensive techniques. There has been agreement on initial confidence-building measures (CBMs) in the Organization for Security Cooperation in Europe (OSCE) and some limited progress on CBMs in the ASEAN Regional Forum and the Organization of American States (OAS). In the UN, we are entering the seventeenth year of negotiation on cybersecurity. There has been the endorsement of general norms, the most important of which embed cyber-attack in the existing framework of international law, including the law of armed conflict. However, there is no agreement to end or constrain the use of cyber-attacks in wartime. Nor is there any agreement on the definition of a "cyber weapon" or what would qualify as the use of force or armed attack in cyberspace. This is unlikely to change, and these areas of disagreement limit the applicability of existing understandings on how to govern armed conflict and make it more difficult to create new ones.

Cyber diplomacy, private or not, raises several questions, including whether it is even useful at this time to pursue negotiations with opponents. So far, there is no indication that there is much room for any negotiated agreement. It may help to differentiate the role of private actors in international cybersecurity. However, while their involvement is politically essential within the community of democracies, the as yet unlearned lesson is that it is not essential in, nor effective for, negotiations between democracies and authoritarian states. The role of private actors in cybersecurity negotiations depends very much on the changed context for internet politics. In the 1990s, when the world seemed to be moving towards consensus on governance and conflict seemed to be in decline, a multistakeholders approach made sense. This is no longer the case in this increasingly conflictual international environment, where authoritarians prefer sovereign counterparts and dismiss or downplay private actors. We should adjust our expectations accordingly.