Working Paper
For circulation at the 2017 Global Digital Futures Forum
May 5, 2017

COLUMBIA|SIPA
School of International and Public Affairs

Normative Restraints on Cyber Conflict

March, 2017

By Joseph S. Nye, Jr.

1. Introduction

Where does the world stand in the development of norms to restrain conflict in cyber space? Elsewhere I have compared learning about cyber security with the way states learned to cooperate in regard to nuclear weapons. ("Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly*, Winter, 2011). While cyber and nuclear technologies are vastly different in their characteristics and effects, at a meta level, the processes of how societies and states learn to cope with a highly disruptive technology have interesting similarities. In terms of chronology, it took states about two decades to reach the first cooperative agreements to limit conflict in the nuclear era. If one dates the cyber security problem not from the beginning of the Internet in the 1970s but from the period since the late 1990s when burgeoning participation made the Internet a substrate for economic and military interdependence (and thus vulnerability), cooperation in cyber is now at about the two decade mark.

The first efforts in the nuclear era were unsuccessful UN centered treaties. In 1946, the US proposed the Baruch plan for UN control of nuclear energy, and the Soviet Union promptly rejected locking itself into a position of technological inferiority. It was not until after the frightening Cuban Missile Crisis, that a first arms control agreement, the Limited Test Ban Treaty was signed in 1963. The NPT followed in 1968 and the bilateral Strategic Arms Limitation Treaty in 1972. In the cyber field, in 1999, Russia proposed a UN treaty to ban electronic and information weapons (including propaganda). With China and other members of the Shanghai Cooperation Organization, it has continued to push for a broad UN based treaty. The US resisted what it saw as an effort to limit American capabilities, and continues to view a broad treaty as unverifiable and deceptive. Instead, the US, Russia and thirteen other states agreed that the Secretary General should appoint a Group of Government Experts (UNGGE) which first met in 2004. It initially had meager results, but by July 2015 it issued a report which proposed norms for limiting conflict as well as confidence building measures that was endorsed by the Group of 20 summit. Groups of experts are not uncommon in the UN process, but only rarely does their work rise from the basement of the UN to a summit of the twenty most powerful states. The success of this group was above the ordinary.

2. The UN Group of Government Experts

The GGE issued reports in 2010, 2013 and 2015 that have helped to set the negotiating agenda for cybersecurity, but despite this initial success, the GGE has limitations. The participants are technically advisors to the Secretary General rather than fully empowered national negotiators, and although their number has increased from the original 15 to 20 to 25, most nations do not have a voice. According to one diplomat who has been central to the process, some seventy countries have expressed interest in participating. But as the numbers expand, the problems of reaching agreement increases. Some observers worry that entropy will set in and they express concern whether this process can continue to succeed.

To understand the GGE, it helps if one puts it in a broader context of normative constraints upon states. The three canonical sources of international law are treaties, customary international law, and expert juridical opinion. Some observers draw a sharp distinction between international law and international norms. The Tallinn Manual, for example, is an important effort by a group of international lawyers to write down what is agreed to be international law. it is clear that lawyers do not always agree, but on many matters they do agree on law that is supposed to be binding on states. A norm, as distinguished from law by Martha Finnemore and Duncan B Hollis,(“Constructing Norms for Global Cybersecurity,” 110 *American Journal of International Law*, 2016) is a collective expectation of proper behavior of actors with a given identity. Norms apply to multiple actors and are not legally binding. “Laws can serve as a basis for formulating norms, just as norms can be codified by law.”(p442) Norms play a role in constituting new roles as well as constraining existing ones. The “oughtness” of their constraints can grow out of law, politics and cultures.

Parsing the differences between laws, norms and other types of constraints is sometimes useful but it is not my purpose here. By lumping together a wide range of normative constraints, I want to illustrate nine potential arenas for action in the following matrix. Horizontally, in terms of formalism, normative constraints on states range from formal treaties to conventional state practice to codes of conduct and norms. Vertically, in scope of membership, the groups thus constrained can range from global, to plurilateral, to bilateral. Such groups can include both states and non-state actors. The totality can also be described as a regime complex.

3. Normative Constraints on States and Non-State Actors

	Agreements	State Practice	Norms and codes
Global	ICANN	Routing practices and exchanges	UNGGE
Plurilateral	Budapest Convention	Like minded groups	G 20, OSCE Regional orgs.
Bilateral	US/China on commercial CNE	Entanglement and self restraint	CBMs, US-Russia hot line

Non-state actors can be constrained by domestic law, punishment, culture, but in a world without overarching international government, why do sovereign states themselves sometimes let normative considerations constrain their behavior? Among the considerations, one reason is fear. Another is external reputation. A third is domestic political pressure.

4. Fear, Prudence and Norms

What can history tell us about the effectiveness of these normative instruments of policy in other areas? In the decade after Hiroshima, tactical nuclear weapons were widely regarded as “normal”, and the U.S. military incorporated nuclear artillery, atomic land mines and nuclear anti-aircraft into its deployed forces. In 1954 and 1955, the Chairman of the Joint Chiefs of Staff told President Dwight Eisenhower that the defense of Dien Bien Phu in Vietnam and the defense of offshore islands near Taiwan would require the use of nuclear weapons, but Eisenhower rejected the advice in part because of fear of unintended consequences. (See my “Deterrence and Dissuasion in Cyber Space,” *International Security*, Winter 2017).

Over time, this prudence developed into a norm of non-use of nuclear weapons which has added to the cost that a decision maker must consider before taking an action to use them. The Nobel Laureate economist Thomas Schelling argued that the development of a norm of non-use of nuclear weapons was one of the most important aspects of arms control over the past 70 years. Ironically, Eisenhower (and other leaders) was unwilling to sign onto a formal norm of no-first use of nuclear weapons because the residual uncertainty of potential use was needed to deter Soviet superiority in conventional forces. It was not until the era of Gorbachev and Reagan that leaders were willing to agree that nuclear war could not be won and must never be fought. The norm of non-use has had an inhibiting effect on leaders of major states, but for new nuclear states like North Korea, one cannot be sure whether the costs of breaking the taboo would be perceived as outweighing the benefits.

In cyber, fear of destroying the benefits reaped from the Internet (which are increasingly important to economic growth) may constrain attacks on the Domain Name System or the IANA function. In addition, the very newness of cyber war and fear of unforeseen consequences in unpredictable systems may contribute to prudence that could develop into a norm of non-use or limited use or limited targets. As Brandon Valeriano and Ryan Manness point out in *Cyber War vs. Cyber Reality* (Oxford University Press, 2015), on a number of occasions when faced with a choice in wartime, political and military leaders have preferred the predictability of kinetic weapons. Sometimes fear of unintended consequences can lead to prudence which can develop into a norm.

5. External Reputation

After World War I, a consensus taboo developed about poisons, and the 1925 Geneva Protocol prohibited the use (though not possession) of chemical and biological weapons. They existed but were not used in World War II because of deterrence through fear of retaliation. Then in the 1970s, two treaties were negotiated that prohibited the production and stockpiling of such weapons. That meant that there is a cost associated not only with their use but even their very possession. Verification provisions for the Biological Warfare Convention are weak (merely reporting to the UN Security Council), and such taboos did not prevent the Soviet Union from cheating by continuing to possess and develop biological weapons in the 1970s. The Chemical Weapons Convention did not stop either Saddam Hussein or Bashir al Assad from using chemical weapons against his own citizens, but they did have an effect on the perceptions of costs and benefits of actions, such as the international dismantling of most Syrian weapons in 2014. With 173 states having ratified the Biological Warfare Convention, states that wish to develop biological weapons have to do so secretly and illegally and face widespread international condemnation if evidence of their activities leak. External reputational harm, along with uncertain benefits in use, appear to be the main reasons that norms seem to have limited possession such weapons.

Normative taboos may become relevant in the cyber realm as well, but not against mere possession of weapons. The difference between a computer program that is a weapon and a non-weapon depends on intent, and it would be difficult to forbid the design, possession, or even implantation for espionage of particular programs. In that sense, cyber arms control cannot be like biological arms control or the nuclear arms control that developed during the Cold War which involved elaborate detailed treaties regarding verification. Unlike physical weapons, it would be impossible to reliably prohibit possession of the whole category of cyber weapons.

A more fruitful approach to normative controls on cyber arms is not to focus a taboo against *weapons* but against *targets*. The United States has promoted the view that the internationally recognized Laws of Armed Conflict (LOAC) which prohibit deliberate attacks on civilians apply in cyber space. Accordingly, the U.S. proposed not a pledge of "no first use" of cyber weapons, but a pledge of no use of cyber instruments against civilian facilities in peacetime.

This approach to norms was adopted by the GGE. The taboo would be reinforced by confidence building measures such as promises of forensic assistance and non-interference with the workings of Computer Security Incident Response Teams (CSIRTs). The GGE report of July 2015 focused on restraint on attacks on certain civilian targets rather than proscription of particular code. At the 2015 summit between American President Barrack Obama and China's President Xi Jinping, the two leaders agreed to set up an expert commission to study the GGE proposal (as well as a separate agreement limiting cyber espionage for commercial purposes). As noted above, the GGE report was endorsed by the leaders of the G-20 and referred to the UN General Assembly. On the other hand, an attack on the Ukrainian power system occurred in December 2015, and was widely attributed to Russia, a GGE member (though Russia might argue that given its hybrid war with Ukraine, it was not bound by a peacetime norm.) Similarly, in 2016, the U.S. accused Russia of using cyber means to interfere in the American election. Despite the fact that the US had added electoral processes as a 17th item on its list of critical infrastructures, Russia clearly did not include the election process in the U.S. as a critical civilian infrastructure covered by the taboo. At this point the development of normative controls on cyber arms remains a slow and incomplete process. In general, the multi-lateralization of norms helps raise the reputational costs of bad behavior. It is worthy of note that the Missile Technology Control Regime and the Proliferation Security Initiative began as voluntary measures and gathered momentum, members, and normative strength over time.

6. Domestic Factors

There is a third process which can lead to statesmen accepting normative constraints on their actions and that arises out of domestic politics. In cyber as in other domains, theorists like Martha Finnemore and Kathryn Sikkink ("International Norm Dynamics and Political Change," *International Organization* 1998) have hypothesized that norms have a life cycle starting with norm entrepreneurs, tipping points into cascades, and then internalization which translate their effects into beliefs that have domestic costs that deter external actions. If one looks at the historical development of norms against the slave trade in the 19th century or in favor of human rights in the second half of the 20th century, one can see that some states are constrained by the effect of norms on domestic opinion. Of course, one would expect such constraints to be stronger in democracies than in authoritarian states (though not totally absent in the latter – witness the effects of Basket Three of the Helsinki Process). Today, in cyber norms the world is largely at the first stage with the GGE as one of a number of important norm entrepreneurs. Perhaps norms are beginning to enter the second phase of a cascade. But the internalization of norms remains weak and limited to narrow elites. Moreover, there is no metric for measuring time in this hypothesized cycle, and indeed no guarantee of a cycle at all. For example, if relations between states become bitter over all, retrogression is certainly possible.

7. Next Steps

There is a wide range of views about the next steps for the GGE process. A first draft of a new report existed at the beginning of this year, but it was a long way from agreement. At the February 2017 Munich Security Conference, the current chair argued that the group should not try to rewrite the 2015 report, but should say more about the steps that states should take in peacetime. Some states suggested new norms dealing with data integrity and maintenance of the core structures of the Internet, but other states believed such expansion would open up a Pandora's box. There was general agreement about more discussion of confidence building measures and of capacity building, but also concern about how states will implement what has already been agreed.

If the GGE norms are to "cascade", states must raise awareness in a broader public. It is noteworthy that the Ukrainian disruption was not flagged and debated as possibly contrary to the GGE report of 2015. A representative of a small country argued that international law was crucial to small states without power, and made the case for more attention to the Tallinn Manual 2.0. The representative of a major power said the GGE should dig deeper on questions such as what is meant by civilian processes. A UN under-secretary argued that the norm development process had to be broadened to include more countries to increase its legitimacy among the 193 UN members, and should relate cyber to other issues such as arms control in space and terrorism. In his view, the 5th GGE should dig deeper and then the 193 members of the UN should debate the report and task the next GGE to examine specific areas.

The GGE process reflects the positions of the states that nominate the experts and their strong views on state sovereignty. Certain normative issues are not discussed. The questions of contents and human rights are finessed by saying that all states agreed to the Universal Declaration of Human Rights though they interpret and implement it in different ways. Further progress on such subjects would probably be limited to plurilateral discussions among like-minded states rather than universal agreements. Other norms that may be ripe for discussions outside the GGE process could include a protected status for the core functions of the Internet; supply chain standards and liability for the Internet of Things; treatment of election processes as protected infrastructure; and more broadly norms for sub-LOAC issues such as crime and information warfare. All these are among the topics that may be considered by the new informal International Commission on Stability in Cyberspace announced by the Dutch Foreign Minister at Munich.

As member states contemplate next steps in the development of cyber norms they are faced with the dilemma of maintaining the effectiveness of the GGE while expanding participation in order to develop a broad legitimacy for norms that will help them to cascade and internalize. The answer may be to avoid putting too much burden of a burden on any one institution like the GGE. Norms are affected by their institutional homes, and in the long run many homes may be better than one. Progress on the next steps of norm formation may require simultaneous use of many of the nine cells for action identified in the matrix above. It will also require a strategy for mutual reinforcement among the cells. For example, the bilateral agreement between China and the US on cyber espionage for commercial purposes was taken up by the G20 as well in bilateral negotiations between China and a number of other states. In some instances, development of norms among like-minded states can lead to norms to which others may accede at a later point. In other instances, norms for security on the Internet of Things may benefit from codes of conduct where the private sector or non-profit stakeholders take the lead. And progress in some areas need not wait for others. The development of a regime complex may be more robust when linkages are not too tight. (See my “The Regime Complex for Managing Cyber Activities,” Research Paper #1, The

Global Commission for Internet Governance, 2014). Such flexibility would be incompatible with an over-arching UN treaty at this point. Expansion of participation is important for the acceptance of norms, but progress on norms will require action on many fronts. We are still in the early stages in the formation of normative constraints on cyber activity.