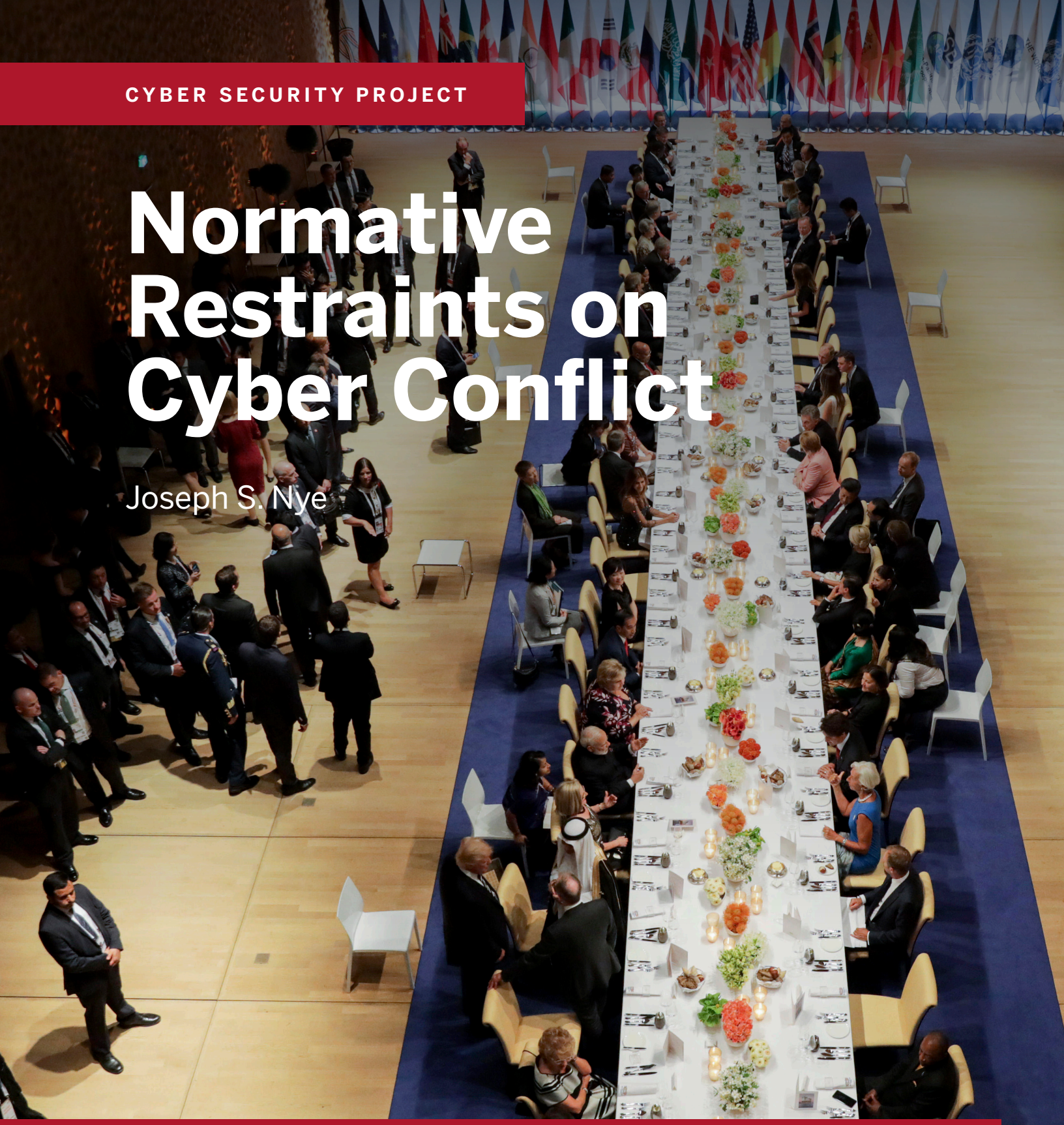
CYBER SECURITY PROJECT

Normative Restraints on Cyber Conflict

Joseph S. Nye



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
AUGUST 2018

Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Originally published in Cyber Security: A Peer-Reviewed Journal Vol. 1, 4 331–342 © Henry Stewart Publications 2398-5100 (2018)

Layout by Mari Dugas

Cover photo: July 7, 2017, the heads of government of the G-20 states and their partners have dinner after a concert in the Elbphilharmonie concert hall in Hamburg, Germany (Kay Nietfeld/ Pool Photo via AP)

Printed in the United States of America

CYBER SECURITY PROJECT

Normative Restraints on Cyber Conflict

Joseph S. Nye

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
AUGUST 2018

Abstract

Cyber security is a relatively new international problem. A decade ago, it received little attention as an international issue, but since 2013 the Director of National Intelligence has named cyber security risks as the biggest threat facing the USA. Although the exact numbers can be debated, various non-profit organisations have listed hundreds of state-sponsored attacks by a score of countries in the past decade. Many observers have called for laws and norms to manage the growing cyber threat. In this paper the author outlines the key normative restraints on cyber conflict. The author draws on the development of international norms in recent history to offer insights into the formation of normative restraints in the cyber realm.

Acknowledgments

This paper is based on an address at the Chinese Academy of Social Science, Beijing, December 2017. I am indebted for comments on an earlier draft to Fadi Chehade, Jack Goldsmith, Andrew Grotto, Trey Herr, Robert Keohane, Alexander Klimburg, James Lewis, John Mallery, and Max Smeets.

Special thanks to Simon Beckett and Henry Stewart Publications LLP for allowing the Belfer Center to reprint this paper. The original print can be access here: https://www.henrystewartpublications.com/csj.

About the Author

Joseph S. Nye is University Distinguished Service Professor and former Dean of Harvard's Kennedy School of Government. He received his bachelor's degree summa cum laude from Princeton University, won a Rhodes Scholarship to Oxford and earned a PhD in political science from Harvard. He has served as Assistant Secretary of Defense for International Security Affairs, Chair of the National Intelligence Council and a Deputy Under Secretary of State. His most recent books include The Powers to Lead, The Future of Power and Presidential Leadership and the Creation of the American Era. He is a fellow of the American Academy of Arts and Sciences, the British Academy and the American Academy of Diplomacy. In a recent survey of international relations scholars, he was ranked as the most influential scholar on American foreign policy, and in 2011, Foreign Policy named him one of the top 100 Global Thinkers. In 2014, Japan awarded him the Order of the Rising Sun.

Table of Contents

1. The Development of the Cyber Security Issue

The term cyber security covers a wide range of problems. Security was not a major concern among the small community of researchers and programmers who developed the Internet in the 1970s and 1980s. In 1996, only 36m people (about 1 per cent) of the world population used the Internet. Within two decades, at the beginning of 2017, 3.7bn people, or nearly half the world population, used the Internet. As the number of users escalated after the late 1990s, the Internet became a vital substrate for economic, social and political interactions. However, along with rising interdependence came not just economic opportunity, but also vulnerability and insecurity. With big data, machine learning and the 'Internet of Things', some experts anticipate that the number of Internet connections may grow to nearly a trillion by 2030. The potential attack surface will expand dramatically and include everything from industrial control systems to heart pacemakers to self-driving cars. The cyber domain will provide opportunities for both private and interstate conflict.

Many observers have called for laws and norms to manage the new international insecurity created by information technology and cyberspace. For example, in 2018 UN Secretary General António Guterres called for 'global rules to minimise the impact of electronic warfare on civilians as massive cyberattacks look likely to become the first salvoes in future wars'.[1] Some doubt this specific scenario, but despite pleas from leaders over the years, the development of norms faces a number of difficult hurdles in the cyber domain. Just to name a few: non-state actors play a major role, some malign and some benign. The Internet is a transnational network of networks, most of which are privately owned, and companies with vast decision spans affect many norms. Unlike the nuclear arena, for example, the cyber domain has multiple stakeholders. Cyber tools can be dual use, fast, cheap and often deniable. Verification and attribution has

been difficult, and barriers to entry are falling. Major states differ in their objectives, with Russia and China stressing the importance of sovereign control and many democracies pressing for a more open Internet. While the Internet is transnational, the infrastructure (and people) on which it rests fall within the differing jurisdictions of sovereign states.

Nonetheless, some norms exist in cyberspace, and the caricature of the world wide web as the 'wild west web' is exaggerated. Elsewhere the author has compared learning about cyber security with the way states learned to cooperate in regard to nuclear weapons.[2] 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 historical 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 international cyber security problem not from the origins of the Internet in the early 1970s but from the period since the late 1990s when it was commercialised, intergovernmental cooperation in cyber is now at about the two-decade mark. Although Moore's law about the doubling of computing power every two years means that cyber time moves quickly, human habits, norms and state practices change more slowly.

The first efforts to develop international norms and institutions to cope with the disruptive new technology of nuclear weapons were unsuccessful UN-centred treaties. In 1946, the USA proposed the Baruch plan for UN control of nuclear energy, but the Soviet Union promptly rejected locking itself into a position of technological inferiority. It was not until after the frightening Cuban Missile Crisis in 1962 that a first arms control agreement, the Limited Test Ban Treaty, was signed in 1963. The Non-Proliferation Treaty followed in 1968 and the bilateral Strategic Arms Limitation Treaty in 1972.

In 1998, Russia first proposed a UN treaty to ban electronic and information weapons (including for propaganda purposes). With China and other members of the Shanghai Cooperation Organization it has continued to push for a broad UN-based treaty. The USA resisted what it saw as an effort to limit American capabilities and continues to view a broad treaty as unverifiable and deceptive. Instead, the USA and 13 other states agreed to a Russian proposal that the UN Secretary General should appoint a group of governmental experts (UNGGE), which first met in 2004. Five GGEs have met within the framework of the UN First Committee Resolution on 'Developments in the Field of Information and Telecommunications in the Context of International Security'. This cumbersome title incorporated both the Russian focus on 'information warfare' and the USA focus on cyber operations.

Initially the GGE process had meagre results, but gradually its members agreed to support a wider process of defining both norms of state behaviour as well as embark on concrete discussions on confidence- building measures. The GGE issued reports in 2010, 2013 and 2015 that helped to set the negotiating agenda for cyber security. In July 2015, it proposed a set of norms that was later endorsed by the Group of Twenty (G20).[3] Groups of experts are not uncommon in the UN process, but only rarely does their work rise from the basement of the UN to being recognised at a summit of the 20 most powerful states. The success of this group was above the ordinary, but it failed to agree on a new report in 2017.

Despite its initial success, the UNGGE had inherent limitations. The participants were technically advisers to the Secretary General rather than fully empowered national negotiators, and although their number increased from the original 15 to 20 to 25, most nations did not have a voice. According to the private estimate of one diplomat, by 2017 some 70 countries had expressed interest in participating.[4] Yet, as the numbers expanded, the problems of reaching agreement increased and extraneous

political considerations weighed more heavily in the deliberations. Some observers expressed doubt that this process could continue to succeed and called for other approaches.

2. Normative Constraints on States

There are several types of normative constraints in international relations. The most familiar is international law which is formal and, by analogy and connection with domestic law, supposedly binding and justiciable. The canonical sources of international law are treaties and customary international law (including expert juridical opinion). Though law has a normative content, some observers draw a sharp distinction between formal international law and less formal international norms. The Tallinn Manuals, for example, represent an important effort by a group of international lawyers to establish a baseline interpretation on how current international law such as the UN Charter, the Geneva Conventions and the Laws of Armed Conflict (LOAC) could be applied to cyber conflict. On some matters the lawyers agreed on the law that is supposed to be binding on state behaviour in cyberspace, but in other areas they differed.[5]

A norm, as distinguished from law by Martha Finnemore and Duncan Hollis, is a collective expectation of proper behaviour 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.'[6] 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. The power of a norm arises from its being shared within a group with which an actor identifies and wishes to enjoy a good reputation. Since there are many groups and many cultures in the multi- stakeholder domain of cyberspace, there are a variety of norms, some shared and some not. The norms that motivate members of the Internet Engineering Task Force, for example, differ from those which move large companies or government security officials or groups on social media.

Norms are supposed to be more binding than principles, which are statements of fact or rectitude that articulate a goal or vision that a group says it wants to achieve. In Finnemore's words, 'In contrast to norms, however, principles are often silent or imprecise about which actors should perform which behaviors to achieve a stated goal'.[7] Principles allow more fudging about behavioural obligations. As aspirations, they can help coordinate public or private actors, but their injunctions often remain vague and subject to multiple interpretations. For example, when Chinese officials told the Fourth World Internet Conference at Wuzhen that China stood for an open Internet subject to sovereignty, they meant something quite different from the principle of an open Internet asserted by the Freedom Online Coalition.

Parsing the differences among laws, norms and other types of constraint can be useful for some purposes, but it is not this paper's intent.[8] In practice, political actors often blur the lines that academic theorists draw between the categories of law, norms, principles and codes of conduct. Lumping a wide range of instruments together in the general category of 'normative constraints' does an injustice to such academic distinctions, but it allows the diversity of potential arenas for normative action to be illustrated in matrix form (see Table 1). Horizontally, in terms of formality, normative constraints range from laws and agreements to common state or private practices to norms, principles and codes of conduct. Vertically, in terms of the scope of membership, the groups thus constrained can range from global to plurilateral (regional or like-minded) to bilateral. Such groups can include both states and non-state actors. This totality of normative restraints is too imperfect to be called an international regime that is characterised as having a clear hierarchical coherence among norms, but elsewhere the author has described it as a regime complex which sometimes consists of inconsistent and overlapping structures.[9]

Non-state actors can be constrained by domestic law, punishment, culture and profit, but in a world without an overarching

international government, why do sovereign states sometimes let normative considerations constrain their behaviour? There are several reasons, and the one that is most obvious and frequently cited is the coordination benefits that arise from sharing common expectations inscribed in law, norms and principles. For instance, states have refrained from serious interference with the domain name system (DNS) that enhances the ability to connect on the Internet and that is overseen by the Internet Corporation for Assigned Names and Numbers (ICANN). And norms and standards for cyber security have been strengthened by the rapid growth in recent years of the cyber insurance market and accounting standards, which illustrates how private actors can supplement governments in the development of norms for coordination of transnational corporate behaviour.[10]

But coordination games are a limited range of state behaviour, and below we shall consider three other factors that may lead states to accept normative restraints on their conflict behaviour: (1) prudence and fear of uncertain consequences; (2) reputational costs to soft power; and (3) domestic political pressure as norms become internalised. These are quite different as causal mechanisms, but that variety can help us to explore the potential and pitfalls for development of norms for cyber security.

Table 1: Normative constraints on states and non-state actors

	Formal agreements	**Common practices**	**Norms, codes, protocols**
Global	UN Charter; LOAC	Routing practices and exchanges; domain name system	UNGGE; ICANN
Plurilateral: like-minded and regional states	Budapest Crime Convention; EU privacy rules	Europol, Interpol; encryption standards	London process; Wuzhen WIC; OSCE, ASEAN, OAS discussions
Bilateral	US/China on commercial espionage	Self-restraint	Hot lines; CSIRT cooperation

3. Uncertainty, Prudence, and Norms

What can history tell us about the effectiveness of normative instruments of policy in other areas? In the two decades after Hiroshima, tactical nuclear weapons were widely regarded as 'normal', and the USA 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 defence of Dien Bien Phu in Vietnam and the defence 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.[11]

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. 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.[12] 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 such as 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 DNS or the Internet Assigned Numbers Authority (IANA) function that is at its core. In addition,

the very newness of cyberwar and fear of unforeseen consequences in unpredictable systems may contribute to prudence and self-restraint that could develop into a norm of non-use or limited use or limited targets. As Brandon Valeriano and Ryan Maness point out, on a number of occasions when faced with a choice in wartime, political and military leaders have preferred the predictability of kinetic weapons.[13] Before sending a pilot across a supposedly destroyed enemy air defence system, a general might prefer the certainty of photographic bomb damage assessment rather than assurances from Cyber Command that the enemy had not recently patched the vulnerabilities in the software of their system.

Experience may shrink the problem of unpredictability, but military lawyers might still want assurances that the software vulnerabilities being exploited would not produce unintended collateral damage such as destruction of the generators of a wide range of hospital systems. As former Director of the Central Intelligence Agency Michael Hayden noted, 'some of these exploits could be pretty ugly so they had to be modified to meet our operational and legal requirements. What we wanted were weapons that met the standards of the laws of armed conflict.'[14] And while some analysts argue that cyber weapons are perishable and must be used quickly in a conflict ('use them or lose them'), others doubt that early use is optimal. For example, early use may disclose and destroy important associated intelligence capabilities needed to manage or end a conflict ('use them and lose them').[15] Or political leaders may realise that cyber penetrations of foreign electric grids and vice versa could produce mutual destruction that would not be to its long-term advantage. Non-action based on uncertainty and self- interest can become salient and develop into a norm.

Sometimes fear of unintended consequences can lead to prudence which over time can produce norms of non-use or limited use. An interesting example with implications for cyber security and the problem of private 'hack-back' is the development of

the regime that put an end to privateering in the 19th century. Egloff argues that it 'can be traced to unintended consequences of state-sponsored and state-tolerated non-state violence'. As governments experienced the difficulties of controlling privateers as well as their negative economic effects, attitudes changed and new norms developed. 'The long-term evolution of security dynamics in a space … becomes more important to the stakeholders over time. An ecosystem of security actors does not change quickly; rather it evolves. Unintended consequences, feedback loops, and conflicting objectives influence how actors' policies change with time. In addition, the concurrent growing importance of the domain to all the actors raises the stakes and creates incentives to stabilize the domain.'[16] As Maurer and others have shown, different states have different attitudes and relationships of control with private proxies in the cyber world, but if the unintended consequences become more clear and costly as states become more dependent on cyberspace, prudence and new norms may evolve.[17]

4. External Reputation and Soft Power

After World War I, there was widespread popular revulsion 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 the European theatre in World War II because of operational difficulties and deterrence through fear of retaliation. In the 1970s, two treaties were negotiated that prohibited the production and stockpiling of such weapons. That stigma created a cost to a country's soft power that became 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. Nor did the Chemical Weapons Convention stop either Saddam Hussein or Bashar al-Assad from using chemical weapons against their 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 chemical weapons in 2014 or the air strike against Syrian chemical weapons in 2017. 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 (loss of soft or attractive power), along with uncertain benefits in use, appear to be the main reasons that norms seem to have limited possession of such weapons.

Normative taboos may become relevant in the cyber realm as well, but not against possession of weapons. There is no popular revulsion against the technology, and some even celebrate it as an instrument of 'bloodless war'. As Schmidle, Sulmeyer and Buchanan have written, no one has been killed by a cyber capability (at least not directly, and not yet).[18] Moreover, unlike

nuclear and biological weapons, cyber technology is inherently dual use. The difference between a computer program that is a weapon and a non-weapon can depend 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 the nuclear arms control that developed during the Cold War and involved elaborate detailed treaties regarding verification of large visible objects. Unlike nuclear 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 and to make use of an existing and well- established international normative structure. The USA has promoted the view that the longstanding norms of discrimination and proportionality incorporated in the internationally recognised LOAC also prohibit deliberate attacks on civilians via cyber instruments. Accordingly, the USA has not pledged 'no first use' of cyber weapons, but has pledged no deliberate use of cyber instruments against civilian facilities contrary to the obligations of humanitarian law. This approach to norms for cyber arms control was adopted by the 2015 GGE report, which also endorsed confidence-building measures such as promises of forensic assistance and non-interference with the workings of computer security incident response teams (CSIRTs). By drawing upon the existing and well-established international norms of LOAC, the 2015 report focused on restraint on attacks on certain civilian targets rather than proscription of particular code.

As noted above, the GGE report was endorsed by the leaders of the G20 and by the UN General Assembly. An attack on part of the Ukrainian power grid occurred in December 2015, however, which was widely attributed to Russia, a GGE member. Similarly, in 2016, the USA accused Russia of using cyber means to interfere in the USA presidential election. After the fact, the USA added electoral processes as a seventeenth item on its list

of critical infrastructures, but Russia clearly did not regard the election process in the USA (or elsewhere) as a critical civilian infrastructure covered by the taboo.

Information warfare (the use of information for hostile purposes) is not new and had been practised by both sides in the Cold War, but cyber technology made it much easier, cheaper, faster and deniable. From Russia's perspective, its troll factories using botnets to manipulate social media and sow mistrust in the American political process was a mere difference of degree, not kind, from the work of American government-funded organisations such as the National Endowment for Democracy operating to question authoritarian practices in Ukraine or Russia. After the 2016 election, it turned out that the political and reputational cost of Russia's cyber intrusions was considerable, as a special prosecutor brought criminal indictments against three Russian companies and 13 civilians, and Russia's relations with the USA remained troubled by the unintended consequences of its actions. But in the absence of a stronger American reaction, it is not likely that the unintended consequences will produce prudence. Whether an agreement on mutual restraint in this arena can be negotiated in the future is debatable because of differences over free speech, but it was clear that the generalities of the 2015 UNGGE report had not solved the problem.

On the other hand, in 2015 China and the USA developed a new norm to restrain their conflict over cyber espionage for commercial purposes. Espionage is a longstanding inter-state practice and not illegal under international law. For years, the USA had pressed China to restrict one aspect of its cyber espionage, the theft of intellectual property and passing it to national companies, and China had resisted. After the American indictment of PLA officers and threat of a disrupted summit, China changed its policy and agreed to the new norm at the September 2015 summit meeting. The norm was later bilaterally extended to a number of other countries.

In general, the multilateralisation of norms helps raise the reputational costs of bad behaviour. It is a slow process but 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. But the process of cyber security norm development might accelerate if there were events or technological developments that increased popular revulsion such as wider loss of privacy, threats to personal safety from developments in artificial intelligence and the Internet of Things, and accidents that involve a significant loss of life.

5. Domestic Politics and Cycles of Internalisation

A third process that can encourage leaders to accept normative constraints on their external actions arises out of domestic politics. Martha Finnemore and Kathryn Sikkink have hypothesised that norms have a life cycle starting with norm entrepreneurs which can be individuals, organisations, social groups and commissions. At a later stage when enough actors in a group characterise behaviour as central to their identity as a member of the group, norms reach tipping points that develop into cascades of acceptance and internalisation, which translate into beliefs that have domestic political costs that deter leaders from some external actions.[19]

The origins of such norms can arise in the evolution of domestic social attitudes or they can be imported. If one looks at the historical development of norms against the slave trade in the 19th century or in favour of human rights in the second half of the 20th century, one can see examples of both. The anti-slavery movement developed strength in the British parliament in the 18th century and led to the abolition of the oceanic slave trade in 1807, which was enforced by the British Navy. Slavery itself was not abolished in the USA until the Civil War, and was not abandoned in Brazil until 1888. But the secessionist Confederacy was unable to obtain official British recognition (which otherwise would have made good realpolitik sense for Britain) because of the internalisation of anti-slavery attitudes in British domestic politics.

Something similar can be seen in the post- World War II human rights movement. The Western victors and their Latin American allies took the lead in promoting a Universal Declaration of Human Rights, but many other states felt obliged to sign on, and subsequently found themselves constrained by American pressure and by concern about their soft power reputations. But

one can also see that some states are constrained by the effect of norms that have become internalised in domestic opinion.[20] 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 which attached human rights to political and economic issues during the Cold War).

Economic pressures in domestic politics could also lead states to internalise norms. As companies find themselves disadvantaged by conflicts of laws relating to privacy and location of data, they may press governments to develop common standards and norms. Similarly, with the rapid growth of the cyber insurance industry, there may be internal pressures for development of standards and norms, for example regarding industrial processors and supervisory control systems embedded in the myriad devices that are becoming connected to the Internet. With time, the early practices of 'build quickly and patch later' may give way to norms and legislation that place more emphasis on security.

With regard to normative restraints on cyber instruments, the GGE was one of a number of important norm entrepreneurs and, along with the First Committee of the UN General Assembly, it may continue to play some role in the future. Perhaps the norms and principles it developed will begin to enter the second phase of a cascade, but the internalisation of these norms remains weak and limited to narrow elites at this point. Popular revulsion and public involvement lags. Moreover, there is no metric for measuring time in this hypothesised cycle, and indeed no guarantee of a cycle at all. For example, if relations between states deteriorate overall, retrogression is certainly possible. This may have been what happened to the GGE between 2015 and 2017. Nonetheless, domestic demands for normative restraints may grow if one considers a longer time scale than just the current decade.

6. Conclusions and Future Steps

One can draw a few modest conclusions and projections from this survey of the development of normative constraints on cyber conflict.

Time: Norms and institutions develop much more slowly than technology, and the process of developing inter-state norms for cyber security is consistent with the time (two decades) that it took for states to develop norms and cooperation in dealing with the disruptive technology of nuclear weapons. While we should think in terms of decades, we should be alert to events and technological surprises that could speed up the process, for example, by developing popular revulsions along the lines discussed above. Moreover, the involvement of multiple stakeholders in negotiations, and not just governments, may broaden public interest and help to accelerate the process, at least in non-authoritarian states.

Values: The early days of the Internet were infused by a utopian libertarian philosophy of a world without borders, but as the Internet became more important, governments began to assert their sovereign control over the parts of the Internet that lay within their borders. This trend is not likely to change. The GGE process reflected the positions of the states that nominated the experts and their strong views on state sovereignty. Authoritarian states have placed particular stress on the norm of sovereignty, but they are not alone. Differences over values have led some analysts to despair about the chances of reaching agreement on global norms. But it is worth remembering that the values gap between the USA and the USSR was even greater during the Cold War but did not prevent development of some agreements. It is interesting to note the first agreements (LTBT and NPT) were focused on the environment and third parties. Bilateral arms control did not come until a decade later. The cyber analogues might be a focus on the basic structure of the Internet and the use of the Internet by criminals and terrorists.

As for the GGE, it is worth noting that certain normative issues were not discussed. The questions of principle regarding content on the Internet and the protection of human rights were finessed by saying that all states agreed to the principles in the Universal Declaration of Human Rights, although they interpret and implement it in different ways. Further progress on such subjects as an Internet Freedom Agenda would probably be limited to plurilateral discussions among like-minded states rather than universal agreements. And even among democratic countries there are important differences over privacy, location of data, and extra-territorial application of principles such as a 'right to be forgotten'. In terms of Table 1, different issues are consistent with different scopes of membership.

Norm entrepreneurship: Norms can be suggested and developed by a variety of entrepreneurs. For instance, a new norm entrepreneur, the non-governmental Global Commission on Stability in Cyberspace was announced by the Dutch Foreign Minister at the 2017 Munich Security Conference and is chaired by former Estonian Foreign Minister Marina Kaljurand.[21] The Commission met before the November 2017 Delhi Conference (the fifth in the so-called London process) and issued a call to protect the public core of the Internet (defined inter alia as routing, the domain name system, certificates of trust, and critical infrastructure). More work is on its agenda.

The Chinese government, using its Wuzhen World Internet Conference series, has issued principles endorsed by the Shanghai Cooperation Organization calling for recognition of the rights of sovereign states to control content on the Internet in their territory, but this need not contradict the call to protect the public core, which refers to connectivity rather than content. Net-mundial, established by Brazil, was an effort to promote multi-stakeholder approaches. Other norm entrepreneurs include the Microsoft Corporation, which has issued a call for a new Geneva Convention on the Internet and an international commission for attribution of the sources of cyberattacks.[22]

The World Economic Forum has useful protocol development networks. Equally important is the development of normative practices regarding privacy and security that are the result of actions by private corporations such as Apple and Facebook regarding encryption, back doors, and principles for the take-down of threatening content regarding child pornography, terrorism, hate speech and false news.

As member states contemplate next steps in the development of cyber norms, the answer may be to avoid putting too much of a burden on any one institution such as the GGE. Norms are affected by their institutional homes and, at this stage, many homes may be better than one or none. Progress on the next steps of norm formation may require simultaneous use of many of the nine cells for action identified in Table 1. It will also require a strategy for mutual reinforcement among the cells. For example, the bilateral agreement between China and the USA 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 principles and practices 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.

Coherence: Multiple norm entrepreneurs and multiple negotiating arenas raises questions about the consistency and coherence of the norms that are developed to restrain cyber conflict. But trying to develop a treaty for the broad range of cyberspace as a whole might turn out to be counter-productive. The loose coupling among issues that now exists permits cooperation among actors in some areas at the same time that they have disagreements in others. For example, China and the USA can use the Internet for economic cooperation even as they differ on human rights and content control. Countries could cooperate

on cybercrime, even while they differ on laws of war or espionage. This might involve agreements not merely to continue existing cooperation through INTERPOL, but also negotiations to forego the use of criminal proxies as a tool of state coercion.

The loosely linked set of norms was described earlier as a regime complex rather than a coherent hierarchical regime. What regime complexes lack in coherence, they make up in flexibility and adaptability. Particularly in a domain with extremely volatile technological change, these characteristics help both states and non-state actors to adjust to uncertainty. Moreover, they permit the formation of clubs or smaller groupings of like-minded states that can pioneer in the development of norms that may be extended to larger groups at a later time. As Keohane and Victor noted of the regime complex for climate change, 'adaptability and flexibility are particularly important in a setting ... in which the most demanding international commitments are interdependent yet governments vary widely in their interest and ability to implement them'.[23] Some have suggested outer space as a model for a cyber treaty. The 1967 Outer Space treaty reserves the use of outer space for peaceful purposes, but technological change has introduced ambiguities in that domain, and cyberspace (which is anchored in sovereign states) fits poorly with models of a global commons such as space or the oceans.[24]

The development of a regime complex may be more robust when linkages are not too tight. Such flexibility would be incompatible with an over-arching UN treaty at this point. There may be other ways to develop linkages among issues and actors that limit the incoherence. For example, Wolfgang Kleinwachter has suggested the model of the 1970s Conference on Security and Cooperation in Europe. He proposes a Conference on Security and Cooperation in Cyberspace that would have four different negotiation arenas ('baskets') that could provide a loose coherence.[25] It might be related to the existing Internet Governance Forum established by the UN in 2005. Other models are possible. Expansion of participation will be 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.

7. Notes and References

1. Khalip, A. (February 2018), 'U.N. chief urges global rules for cyber welfare', Reuters, available at https:// mobile.reuters.com/article/amp/idUSKCN1G31Q4 (accessed 12th March, 2018).

2. Nye, J. S. (Winter 2011), 'Nuclear Lessons for Cyber Security', Strategic Studies Quarterly, Vol. 5, No. 4, pp. 18–38.

3. United Nations (July 2015), 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/70/174, available at http://undocs.org/A/70/174 (accessed 12th March, 2018).

4. Personal communication with UN official, February 2017.

5. Schmitt, M. N. (ed.) (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge; and Schmitt, M. N. (ed.) (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge.

6. Finnemore, M. and Hollis, B. (July 2016), 'Constructing Norms for Global Cybersecurity', The American Journal of International Law, Vol. 110, No. 3, p. 442.

7. Finnemore, M. and Hollis, B. (November 2017), 'Cybersecurity and the Concept of Norms', Carnegie Endowment for International Peace. Finnemore builds succinctly on the political science theories of international regimes pioneered by John Ruggie, Robert Keohane and Stephen Krasner among others two decades ago.

8. For an excellent example, see Tikk, E. and Kerttunen, M. (2017), The Alleged Demise of the UN GGE: An Autopsy and Eulogy, Cyber Policy Institute, The Hague.

9. See Nye, J. S. (2014), 'The Regime Complex for Managing Cyber Activities', The Global Commission for Internet Governance, Paper Series, 1.

10. I am indebted to Trey Herr for discussion of cyber insurance. See also, Morgus, R. (2016), "Cyber Insurance: A Market Based Approach to Information Assurance," in Harrison, R. and Herr, T., Cyber Insecurity, Rowman and Littlefield, London, pp. 155–170.

11. Nye, J. S. (Winter 2017), 'Deterrence and Dissuasion in Cyber Space', International Security, Vol. 41 No. 3, pp. 44–71.

12. Schelling, T. (2006), 'An Astonishing 60 Years: The Legacy of Hiroshima (The Nobel Lecture)', PNAS, Vol. 103, No. 16, 6089–6093, available at http:// www.pnas.org/content/ pnas/103/16/6089.full.pdf (accessed 12th March, 2018).

13. Valeriano, B. and Maness, R. (2015). Cyber War vs. Cyber Reality, Oxford University Press, Oxford.

14. Hayden, M. V. (February 2014), 'The making of America's cyberweapons', Christian Science Monitor, available at, https://www.csmonitor.com/World/ Passcode/ Passcode-Voices/2016/0224/The-making- of-America-s-cyber-weapons (accessed 12th March, 2018).

15. Smeets, M. (2018), 'A Matter of Time: On the Transitory Nature of Cyberweapons', Journal of Strategic Studies, Vol. 41, Nos. 1–2, pp. 6–32

16. Egloff, F. (2017), 'Cybersecurity and the Age of Profiteering', in Perkovich, G. and Levite, A. (eds), Understanding Cyber Conflict: 14 Analogies, Georgetown University Press, Washington, pp. 236, 243.

17. Maurer, T. (2018), Cyber Mercenaries: The State, Hackers and Power, Cambridge University Press, Cambridge.

18. Schmidle, R. E., Sulmeyer, M. and Buchanan, B. (2017), 'Non-Lethal Weapons and Cyber Capabilities', in Perkovich, G. and Levite, A., Understanding Cyber Conflict: 14 Analogies, Georgetown University Press, Washingtonp.31

19. Finnemore, M. and Sikkink, K. (September 1998), 'International Norm Dynamics and Political Change', International Organization, Vol. 52, No. 4, pp. 887–917.

20. Simmons, B. (2009), Mobilizing for Human Rights: International Law in Domestic Politics, Cambridge University Press, Cambridge.

21. In full disclosure, I am a member of the Commission.

22. See Smith, B. (2017), 'The Need for a Digital Geneva Convention', Keynote Address at the RSA Conference 2017, available at https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address- at-the- RSA-Conference-2017.pdf (accessed 12th March, 2018).

23. Keohane, R. O. and Victor, D. (2010), 'The Regime Complex for Climate Change', Perspectives on Politics, Vol. 9, p. 8.

24. Meyer, P. (2016), 'Outerspace and Cyberspace: A Tale of Two Security Realms', in Osula, A. M. and Roigas, H. (eds), International Cyber Norms: Legal, Policy and Industry Perspectives, NATO CCDCOE, Tallin, pp. 155–169

25. Kleinwachter, W. (January 2018), 'Towards a Holistic Approach for Internet Related Public Policy Making', Global Commission of the Stability Cyberspace, GCSC Thought Piece.

Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Printed in the United States of America