International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches

Fahad Nabeel[*]

Abstract

In recent years, several states have developed cyber capabilities being used against rival states. The rapid weaponisation of cyberspace has entered the fifth domain of warfare wherein states engage in short of war battlefield. The absence of international rules to deal with cyber arms race is aggravating the cyber landscape. A number of challenges identified are a hindrance towards an international cyber regime. Similarly, experts remain divided on what approach should be adopted to deal with threats from the cyber domain. The paper investigates the approaches of leading cyber advanced countries, the United States, China and Russia towards establishing an international cyber regime. Despite differences in the cyber domain, the three countries face common threats which can serve as the basis for cooperation in the establishment of an international regime.

Keywords: China, Cyber Warfare, International Cyber Regime, Russia, United States

[*] Fahad Nabeel is an M.Phil. scholar in International Relations at the National Defence University, Islamabad. He is a Research Associate at the Centre for Strategic and Contemporary Research.

Introduction

Modern information and communications technology have served as the physical infrastructure that has truly connected countries all across the world into a global village. The technologies that have transformed everyday life by bringing innovations in various sectors have also been used against government and private entities for destructive purposes.

For more than a decade, there has been an increase in the manifestation of states' capabilities to cause harm to its enemies through the use of modern Information and Communications Technology (ICT). Prior to the invasion of Iraq in March 2003, the United States (US) undermined the political and military defences of Saddam's regime by preemptively cutting off Iraqi computer networks and internet grid.[1] In September 2007, Syrian air defence systems were hacked by Israel to blind the former against the incoming attack in the form of jets bombing a suspected nuclear site in Diaya-al-Sahar.[2] Later that year, Stuxnet, a sophisticated malware was launched by the US and Israel to shut down a nuclear reactor in Iran's Natanz. In early 2014, Barack Obama ordered cyber-strikes against the North Korean missile program to sabotage test launches.[3] Other notable cyberattacks which occurred over the past decade include Titan Rain in 2003, Russian attacks targeting Estonia in 2006 and Georgia in 2008, WannaCray and NotPetya in 2017.[4]

Within the past decade, leading up to early 2018, an estimated 200 known cyberattacks targetting states have been carried out. The targets of these attacks ranged from military defence systems to power grids. Currently more than 30 states have the capability to conduct cyberattacks.[5] Cyber weapons' armed states engage in a low-level, short of war conflict. There is a realisation to keep

[1] Ilai Saltzman, "Cyber posturing and the offense-defense balance," *Contemporary Security Policy 104,* no. 1, (2013): 40-63.

[2] George Lucas, *Ethics of Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* (Oxford: Oxford University Press, 2017).

[3] David E. Sanger and William J. Broad, "Trump inherits a secret cyberwar against North Korean missiles," *New York Times*, last modified March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-koreamissile-program-sabotage.html.

[4] Mariarosaria Taddeo, "Deterrence and Norms to Foster Stability in Cyberspace," *Philosophy & Technology 31,* no. 3, (2018):323–329.

[5] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown Publishing Group, 2018).

it this way in order to avoid military confrontation. The absence of international rules or norms to govern international conflict in what has been described as the fifth domain of warfare, the other four including land, water, air and space, is aggravating the cyber landscape.

A number of experts believe that it is impossible to have an international cyber convention. Such measures should be the basis of an international cyber regime. This is mainly due to the rapid technological changes which bring new challenges to the domain and the issue of verifiability. However, they prefer to limit chances of direct conflict through reliance on informal cooperation and strategic deterrence. Contrarily, some experts agree that achievement of effective arms control in the cyber domain has been met by a number of challenges. However, they draw their inspiration for formulating an international cyber convention by pointing out to history which witnessed the introduction of a number of international arms control treaties or agreements in the 20th century.

New cyber technologies have sparked an international cyber arms race which continues to weaponise cyberspace. History remains witness to the fact that the previous international arms race was contained through international diplomacy which resulted in formal multilateral agreements. Through out the evolution of weaponry from guns and bullets to nuclear weapons, the international community has remained engaged to contain and limit the use of weapons. Consequently, it contributed to reducing fear and tension, increasing transparency and the reciprocal reduction of arms. Therefore, it is necessary that an international cyber regime should be formulated by the global community to ensure that cyberspace does not become a war theatre.[6]

The formation of the international cyber regime will help in addressing some of the key issues faced by governments and academicians while formulating effective cyber deterrence. These issues include: difficulty of attributing cyber operations, difficulties faced in distinguishing hostile attacks from involuntary mistakes, lack of clarity regarding which cyberattack falls under the purview of international law and lastly lacking credibility of rational threats.

[6] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology 31,* no. 3, (2018): 379-407.

Historical Background

Despite the ever increasing threats originating from the cyber domain, currently there is no international cyber regime to deal with cyber related threats. However, there exist a few treaties which address certain cybersecurity issues. In this regard, the two main international agreements are the Budapest Convention on Cybercrime in 2001 (followed by its 2006 Additional Protocol) and the Shanghai Cooperation Organisation's (SCO) International Information Security Agreement in 2009. Both these agreements are severely limited in terms of scope and membership.

In 2013, the Tallinn Manual on the International Law Applicable to Cyber Warfare emerged as an outcome of cyber governance discussions in Estonia. The manual formulates how *jus ad bellum*, international humanitarian law (IHL) and laws of state responsibility apply in cyber context. However, the utility of the manual to de-escalate cyber conflict is modest because of and not exclusive to the following three reasons: failure to gain wider support, limited interpretation of how existing laws may apply, and inadequacy of an agreement even if all states agree on the general applicability of *jus ad bellum* and IHL.[7]

In 1998, Russia proposed a United Nations (UN) treaty to ban electronic and information weapons. It, along with other members of the SCO, has continued to push for a broad UN based treaty. The Russian proposal that the UN Secretary General should appoint a Group of Governmental Experts (UN GGE) was agreed by the US and 13 other states. The group met for the first time in 2004.

To incorporate Russian focus on information warfare and the US focus on cyber operations, five UN 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. Initially, the UN GGE process produced meagre results but gradually its members agreed to support a wider process of defining norms of state behaviour and embarking on concrete discussions on confidence building measures. The group issued reports in 2010, 2013 and 2015 that helped in setting the negotiating agenda

[7] George Lucas, *Ethics of Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* (Oxford: Oxford University Press, 2017).

for cybersecurity. In July 2015, UN GGE earned a rare achievement when the Group of Twenty (G20) endorsed a set of norms proposed by the UN GGE. Nevertheless, the group failed to agree on a new report in 2017.

Despite its initial success, the UN GGE faced some limitations. The participants were technically advisers to the Secretary General but were not entitled to participate in national negotiations. Most nations did not have a say in the process. According to one estimate, approximately 70 countries showed interest in participation by 2017. The problems of reaching an agreement increased with expanding numbers. Lastly, with increasing participants, extraneous political considerations weighed more heavily in the deliberations. Because of the aforementioned limitations, some observers doubt the success of the process and call for alternative approaches.[8]

Challenges for an International Cyber Regime

Apart from the efforts undertaken to pursue an international cyber regime, a number of challenges have been identified regarding the failure to materialise it, which are as follows:

i. Impossible to implement monitoring and enforcement mechanisms

The most common objection in the pursuance of an international cyber regime is the issue of monitoring and enforcement mechanisms. A number of experts say that it will be impossible to gauge compliance or enforcement of agreements related to the cyber domain. Due to their dual-use and concealed nature, implementing monitoring and enforcement mechanisms for cyber weapons will be difficult.

Mette Eilstrup-Sangiovanni argues that the challenge of monitoring compliance appears to be less of an obstacle towards cooperation in the cyber domain. The reason for such an assertion is that formulating a reliable verification of compliance within an international cyber convention should be *exante* (weapons development and possession) rather than *ex-post* (weapons use).[9]

[8] Joseph Nye, "Normative Restraints on Cyber Conflict," *Cybersecurity: A Peer-Reviewed Journal 1,* no. 4, (2018).

[9] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology 31,* no. 3, (2018): 399.

ii. Negotiating any cyber convention would take took long

The second major objection is that it will take too long to negotiate an international cyber convention. A number of experts believe that negotiating treaties is a long and cumbersome process which makes them unsuitable to cybersecurity and internet governance due to rapid technological changes. A review of international treaty negotiations indicates that international norm creation and acceptance is generally a slow process. However, formal treaty negotiations accelerate the process and also add political weight and transparency to the issue. Therefore, embarking on negotiations will have a positive impact towards the long journey of materialising an international cyber convention.[10]

iii. A cyber convention would be insufficient in adapting to rapid technological changes

The third objection is that any cyber convention would become outdated due to rapid technological changes. However, counterarguments to the objection are presented through the indication that nearly all spheres of international arms control have to face problems of unpredictable technological advances. An example can be taken of the Chemical Weapons Convention (CPC). Since its inception in 1993, CPC has undergone periodic updating of verification annexes and lists of prohibited substantives due to new developments in the chemical industry.

Moreover, many international arms control agreements have periodic review conferences which allow governments to update terms of agreement. Since enforcement of the Biological Weapons Convention (BWC) in 1975, state parties to the convention have held seven review conferences, mostly focusing on strengthening verification and reviewing the Convention in light of new scientific and technological developments.

Therefore, an international cyber convention will not be perfect when first formulated and will be subject to several revisions in future. The problem of adaption to rapid technological changes can also be addressed through prohibition of specific behaviours like the use of cyber weapons against civilians

[10] Ibid.

rather than banning development or possession of entire categories of weapons technology.[11]

iv. It is still too early to negotiate an international cyber convention

The fourth objection implies that it is too early to negotiate an international cyber convention which will govern cyberwarfare. Some scholars argue that historically, treaties governing new weapons technologies have often been crafted only after the technologies have been in use for some time.[12] The examples of such treaties are conventions that govern anti-personnel landmines and cluster munitions. The reason for such a delay in formulating a treaty, as identified by scholars, is that states are generally hesitant in restricting the use of weapons that can be of advantage to them on the battlefield until they have acquired sufficient experience to weigh the precise costs and benefits of doing so. Therefore, scholars believe that states will meaningfully pursue an international cyber convention only when they became familiarised with emerging technologies and practices. In brief, the point of arms control agreements is simply to cement current state practice.

However, Mette Eilstrup-Sangiovanni argues that states have often been a great deal more ambitious as reflected in the adoption of the Outer Space Treaty in 1967 and the Environmental Modification Convention (ENMOD) of 1977. These treaties constitute a far-sighted bargain among states to prevent horrific threats to mankind that have been made possible by emerging technologies which, not fully matured have been put to use. A similar far-sighted agreement is now required to govern the conduct of states in cyberspace.[13] Contrarily, Joseph Nye argues that technological transformation has introduced ambiguities in the space domain and the models of global commons like space do not fit with cyberspace; which remains anchored in national policies of sovereign states.[14]

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Joseph Nye, 'Normative Restraints on Cyber Conflict," *Cybersecurity: A Peer-Reviewed Journal 1,* no. 4, (2018).

v. A formal treaty will be too constraining for states

The formal nature of an international convention governing cyberspace is also an objection. A review of international arms control agreements indicates that agreements take many forms. Some agreements are highly specific and obligatory whereas other agreements have no central monitoring, verification or compliance apparatus. Several experts call for closer international cooperation on cybersecurity which should be based on loose norms and voluntary guidelines. They believe that the soft law approach will stand a greater chance of success rather than attempts at imposing formal legislation. However, Mette Eilstrup-Sangiovann argues that a precisely codified and legally binding treaty governing cyber conflict is needed due to the involvement of a large number of direct stakeholders in the cyber domain. To address the verifiability problem, states need to foster robust norms of prohibition against cyberattacks in addition to ensuring compliance at the domestic level.[15]

vi. Only highly committed states will be willing to become parties to a formal treaty

Another major objection is that only a few highly committed states will become willing to adhere to binding rules. Therefore, a wide range of incentives need to be offered to states so that they become party to an international convention. The incentives that can be offered can be intelligence sharing, joint mechanism for attribution, technical assistance and funding, joint disaster response, and establishing a multilateral fund for recovery and reconstruction to help states which face cyberattack. [16]

In addition to these six major objections, there are other difficulties towards the formulation of developing norms which include a major role played by non-state actors and private owners of most transnational networks, collectively combining into the internet.[17]

Approaches of Great Powers towards an International Cyber Regime

[15] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology 31,* no. 3, (2018): 402.

[16] Ibid.

[17] Joseph Nye, "Normative Restraints on Cyber Conflict," *Cybersecurity: A Peer-Reviewed Journal 1*, no. 4, (2018).

In this section, the approaches of the three countries on various aspects of any future international cyber regime will be discussed.

i. Defining Cyberspace

Cyberspace is simply defined as a man-made environment consisting of information/data and ICT control infrastructure. The US Department of Defense has defined cyberspace as, 'A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure.'[18] However in a number of other documents, cyberspace is generally defined as a 'global domain within the information environment consisting of the interdependent network of information system infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers'.[19]

Surprisingly, Chinese cyber strategy documents have not defined the term cyberspace. On the other hand, Russian policymakers constitute cyber operations under the broader framework of information warfare which encompasses computer network operations, electronic warfare, psychological and information operations. Therefore, cyber related terms are not mentioned in their strategy documents.[20] Nevertheless, both Russia and the US defined cyberspace under the 2013 cybersecurity pact as 'An electronic medium through which information is created, transmitted, received, stored, processed and deleted'.[21] In short, the US is the only country among the three that has either defined cyberspace in its strategy documents or under a bilateral pact.

ii. Defining Cyber Warfare

Though the general definition is very broad, according to current literature, the term cyber warfare is generally defined as 'any hostile act that occurs in or

[18] "The National Military Strategy for Cyberspace Operations (U)," *National Security Archive*, last modified December 2006, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

[19] *Glossary of Key Information Security Terms*, eds. Richard Kissel, National Institute for Standards and Technology, US Department of Commerce, NISTIR 7298, Revision 2, - 2010.

[20] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA*, last modified March 2017, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

[21] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher et al., "Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity," *EastWest Institute*, last modified February 2014, https://www.files.ethz.ch/isn/178418/terminology2.pdf.

through cyberspace'. Joseph Nye observes that there are only a few hostile and criminal acts that escalate to acts of war. Therefore, there is a need to identify acts that should constitute as acts of war.[22]

The US is the only country which, as with cyberspace, has defined cyber warfare in its strategy documents and under a bilateral agreement. The American documents have defined cyber war as 'The use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems'.[23] Under the 2013 cybersecurity pact with Russia, cyber war is defined as, 'An escalated state of cyber conflict between or among states in which cyberattacks are carried out by state actors against cyber infrastructure as part of a military campaign. Cyber wars can be declared (formally declared by an authority of one of the parties) or de facto ones (with the absence of a declaration)'.[24] However, both countries have defined cyber warfare as 'Cyberattacks that are authorized by state actors against cyber infrastructure in conjunction with government campaign'.[25]

iii. Defining Cyber Weapons

The joint US-Russia cybersecurity pact defines cyber weapons as a, 'Software, firmware or hardware designed or applied to cause damage through the cyber domain'.[26] The dual-use nature of various cyber technologies makes it highly difficult to distinguish between offensive and defensive cyber capabilities. For example, the US and China collectively have a majority of military units that are responsible for cybersecurity and possess both offensive and defensive cyber capabilities.

iv. Cyber Governance

In terms of cyber governance, all three countries are divided into two camps.

[22] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology 31,* no. 3, (2018): 382.

[23] Bryan Christiansen and Fatmanur Kasarcı, *Corporate Espionage, Geopolitics, and Diplomacy Issues in International Business* (Pennsylvania: IGI Global, 2016), 60.

[24] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher et al., "Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity," *East West Institute*, last modified February 2014, https://www.files.ethz.ch/isn/178418/terminology2.pdf.

[25] Ibid.

[26] Ibid.

China and Russia advocate a multilateral model in which only states interact with each other and make decisions about policy and permissible actions in the cyber domain. This model allows a greater regulation of information by states and excludes private entities from having their say in cyber related matters. The SCO, whose members include both China and Russia, has presented this model in the proposed Cyber Code of Conduct.

Contrarily, the US, along with its allies, has endorsed a multi-stakeholder model which advocates inclusion of all appropriate stakeholders. Along with governments, the model advocates inclusion of the private sector, civil society, academia and individuals. By definition, this model excludes the existence of any international treaty. However, further elaboration of globally accepted norms is necessary for the peaceful conduction of activities in the cyber domain.[27]

The US hostility towards binding international rules is mostly due to its technological superiority especially in the realm of tactical electronic warfare which strong states incentivise for maintaining maximum freedom of action in the cyber domain. The American decision makers fear that acceptance of binding international rules will constrain its conduct and will allow other states to rapidly enhance their capabilities against the US.

China envisions a world of government controlled national internets and wants to weaken the bottom-up, private sector led model of internet governance championed by the US and its allies. By allowing the UN to play a larger role in internet governance, Chinese policymakers believe they would have a large say in regulating ICT and formulating the global rules for cyberspace.[28] Russia advocates the UN Charter based rules in cyberspace by emphasising on respect for national sovereignty and non-interference in internal affairs.[29]

v. Objectives

The US is concerned about securing computer networks along with providing open and secure internet for free flow of information and freedom of expression.

[27] Ilona Stadnik, "What is an International Cybersecurity Regime and how we can achieve It?," *Masaryk University Journal of Law and Technology 11,* no. 1, (2017): 129-154.

[28] Adam Segal, "When China Rules the Web," *Foreign Affairs 97 ,* no. 5, (2018): 10-18.

[29] Joyce Hakmeh, "Cyberattack Revelations Appear to Undercut Russia's UN Efforts," *Chatham House*, last modified October 10, 2018, https://www.chathamhouse.org/expert/comment/cyberattack-revelations-appear-undercut-russia-un#.

To protect the current status quo in the cyber domain, America is building up its offensive cyber capabilities. On the other hand, Russia and China place high priority on information security and combating threats to the society, the political regime and the stability of a state. Terrorism, extremism and separatism are also viewed as other major threats.[30]

vi. Role of Private Entities in Internet Governance

Currently, some of the most important political and technical decisions concerning the global internet are formulated through a multi-stakeholder model which involves government representatives, engineers, members of non-profit organisations, lobbies and individuals. For example, Internet Engineering Task Force (IETF) is essentially responsible for the explanation of technical standards. Similarly, Internet Corporation for Assigned Names and Numbers (ICANN) manages the Domain Name System (DNS).

China, along with several developing countries, remains critical of these organisations and views them as instruments in favour of American and Western hegemony. China seems to be trying to make the Internet Governance Forum (IGF) more intergovernmental and put it more clearly under the responsibility of the UN.[31] According to the 2010 White Paper on the internet in China, the UN is viewed as the ideal framework for a global internet governance. Similarly, both China and Russia support giving International Telecommunications Union (ITU) responsibilities for defining policy for internet governance.

Russia has long criticized the institutional construct of the Internet Assigned Numbers Authority (IANA). The main criticism revolves around the two critical layers of the global internet infrastructure which are controlled by US based corporations, which remain accountable to the American Government. For more than a decade, China and Russia, along with Brazil and India, have been pressing for a revised model and for the internationalisation of the IANA. They emphasise on IANA to become an intergovernmental organisation, which would be linked to the UN. The ITU has been repeatedly proposed as an alternative to

[30] Ilona Stadnik, "What is an International Cybersecurity Regime and how we can achieve It?" *Masaryk University Journal of Law and Technology 11,* no. 1, (2017): 129-154.

[31] Séverine Arsène, "*The impact of China on global Internet governance in an era of privatized control,"* (Chinese Internet Research Conference, Los Angeles, United States, May 2012).

manage IANA functions.[32]

vii. Internet sovereignty

Although the internet is transnational, the infrastructure and the users fall within the jurisdictions of sovereign states. Both Russia and China stress on the importance of sovereign control whereas the US presses for a more open internet.[33] The 2010 White Paper of Internet in China clearly states that the Chinese Government should control internet infrastructure, regulations and codes of conduct.[34] According to the 2015 plan by Institute for Internet Development (IID), Russia views internet sovereignty as 'an adequately high level of self-sufficiency and technological independence'.[35]

viii. Cyber enabled information warfare

Cyber technology has made information warfare easier, cheaper, faster and deniable. From a Russian perspective, it deployed troll factories, manipulating narrative on social media. Sowing mistrust in the American political process during the 2016 elections was similar to the working of American Government-funded organisations operating to question authoritarian practices against Russia. The Russian interference in the presidential election led to a more troubled relationship between the two countries. Nevertheless, the absence of a stronger American response to the election interference did not lead towards a more prudent policy. Difference over the interpretation of free speech remains the most contentious issue towards agreeing on mutual restraint.[36]

ix. Cyber Espionage

For the past several years, the US has pressed China to restrict theft of intellectual

[32] Oleg Demidov and Alexandra Kulikova, "Global Internet Governance and International Security in the field of ICT use," *PIR Press*, last modified 2015, http://pircenter.org/media/content/files/13/14340274400.pdf.

[33] Joseph Nye, "Normative Restraints on Cyber Conflict," *Cybersecurity: A Peer-Reviewed Journal 1,* no. 4, (2018).

[34] "Protecting Internet Security," *China.org.cn*, last modified June 8, 2010, http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm

[35] "The Internet in China," *China.org.cn*, last modified June 8, 2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm

[36] Joseph Nye, "Normative Restraints on Cyber Conflict," *Cybersecurity: A Peer-Reviewed Journal 1,* no. 4, (2018).

property, one of the several aspects of Chinese cyber espionage, but China has resisted American attempts. However, China reversed its policy and both countries in September 2015 agreed to develop a new regulation that calls for restraining their conflict over cyber espionage for commercial purposes. Later on, China bilaterally extended this norm to a number of countries including the G20 countries.[37]

Cyber Crimes

The US is a signatory to the Budapest Convention signed in 2001, though China and Russia are not party to it. Both China and Russia refuse to ratify the Budapest Convention because they did not participate in the drafting process and because they claim that the convention infringes on their sovereignty. Instead, Russia has been advocating a UN global treaty on cybercrime for several years. However, the Russian proposal remains blocked by the US and the EU states.[38] On the other hand, China promotes adoption of the SCO issued International Code of Conduct for Information Security. The code discourages interference in the internal affairs of states through ICT and curbs information that incites terrorism, separatism or extremism.[39]

Threat Perceptions

In terms of threat perceptions, Russia and China are closer to each other. Both countries put an emphasis on sovereignty in cyberspace. However, the US is concerned with network security and free flow of information for economic and political reasons. The commonality of issues that these three countries regard as dangerous for national security include the use of ICT for terrorism, cybercrime, threats to safe and stable functioning of the global and national critical information infrastructures, and lastly cyberattacks on the national critical infrastructure and industrial control systems.[40]

[37] Adam Segal, "The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement," *Council on Foreign Relations*, last modified January 4, 2016, https://www.cfr.org/blog/top-five-cyber-policy-developments-2015-united-states-china-cyber-agreement.

[38] Joyce Hakmeh, "Building a Stronger International Legal Framework on Cybercrime," *Chatham House*, last modified June 6, 2017, https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime.

[39] Ron Cheng, "Prospects for U.S.-China Cybercrime Cooperation: The Road Thus Far," *Lawfare*, last modified March 9, 2017, https://www.lawfareblog.com/prospects-us-china-cybercrime-cooperation-road-thus-far.

[40] Ibid.

Way Forward

Given the troubled nature of their relationship especially following the Russian interference in the US presidential elections of 2016, any breakthrough in reaching new agreements between the two countries seems impossible in the near future.

The US and Russia, the two most advanced cyber powers, need to restart their dialogue on cyber issues. The American administration can initiate dialogue with Russia on cyber issues in the same fashion as it reached out to China. In 2015, the Obama administration was close to imposing broad sanctions on China following the hacking of industrial secrets by hackers allegedly backed by the Beijing regime. However, Obama and Xi Jinping were able to sign a substantial Cyber Economic Espionage agreement which curtailed Chinese cyberattacks on the US. Therefore, the US and Russia should strive for a realistic and limited in scope agreement inclusive of preventing dangerous military activities in cyberspace.[41]

Apart from bilateral negotiations between the US and Russia, loose coupling among issues should be encouraged. This allows states to cooperate in some areas while holding on to disagreements in other areas. For example, the US and China can strengthen economic cooperation through the internet while differing on human rights and content control.[42]

The literature on international cyber regime comprises of various frameworks and proposals to formulate an international cyber regime. An international regime can articulate clear and binding rules and norms that will distinguish lawful and unlawful behaviour and also facilitate in punishing cyber aggressors. However, Mette Eilstrup-Sangiovanni argues that the success of those rules and norms will depend on the fulfilment of four criteria at the least. Firstly, the convention must offer sufficient positive incentives to ensure broad participation of states. Secondly, such rules should be formulated which should not only constrain behaviour but also be practically implemented keeping in

[41] Elena Chernenko, Oleg Demidov and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," *Council on Foreign Relations*, last modified February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

[42] Joseph Nye, "Normative Restraints on Cyber Conflict," *Cybersecurity: A Peer-Reviewed Journal 1,* no. 4, (2018).

view the current technology. Thirdly, the convention must provide sufficient credible information to reduce uncertainty about state interests and enable effective signalling. Finally, the convention should ensure that non-compliance will result in significant costs.[43]

In cyber context, it is not easy to observe or infer capabilities and motivations of states. The unavailability or the use of meaningless tools that help in understanding the signalling of the necessity of the states, having formal rules will help in distinguishing permitted and prohibited behaviour. Formulation of rules will help in lessening ambiguity about the intentions of a state that is planning to violate a binding international agreement. Similarly, the binding nature of an agreement will help in knowing whether states intend to adhere to the rules or not.

Unlike certain conventional and non conventional weapons, it would be practically difficult to impose certain restrictions on cyber weapons. As discussed earlier, the dual-use nature of various cyber technologies will make it difficult to agree on what constitutes a cyber weapon prior to deployment. However, an international agreement can focus on restricting use of cyber weapons by banning use of those weapons against certain targets like civilians, healthcare, etc. Similarly, it will also be important to clearly formulate rules which not only permit and justify cyber intrusion but also explain what constitutes an act of aggression.

An important aspect which the international cyber regime needs to address is the occurrence of unintended conflict due to cyber accidents. This can be done by formulating crisis management mechanisms. In the cyber domain, it is very difficult to identify a cyber accident from an overt hostile act. Similarly, it cannot be concluded as to whether a non-state actor who launched a cyber operation against a victim state was doing so on its own or was supported by the state from whose territory the attack was launched. Therefore, it is important to establish strong channels of communication and institute obligatory early warning mechanism through which states agree to notify each other immediately in case of the detection of any attack launched from their territory.[44]

[43] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology 31,* no. 3, (2018): 391.

[44] Ibid.

The attribution is a key issue which needs to be addressed by the international cyber regime. Existing international law cannot be applied to an individual who conducts a cyberattack on his/her own. However, the host country can either prosecute the individual through its own laws or extradite him/her to the victim state through the extradition process. This can prove to be difficult. For example, the American authorities have failed to extradite alleged Russian hackers from European countries.[45]

Despite long-held pessimism about addressing the attribution issue, many experts are now of the opinion that attribution of large-scale attacks against critical infrastructure can be done at least if adequate time and resources are available. In short, reliable attribution is time consuming and costly. Therefore, a number of proposals have been proposed to deal with the said issue.

First, a joint attribution mechanism should be created by pooling technical and financial resources. This will help in providing reliable attribution at lower cost to many states, who cannot afford technical capabilities to study data for attribution. It will also prove beneficial because of the involvement of several states in uncovering the forces behind cyberattacks and retaliate against them. Joint attribution will enhance the overall credibility of retaliatory threats.

In this regard, the International Monitoring System (IMS) of Comprehensive Nuclear-Test-Ban Treaty (CTBT) is presented as a model. Once enforced, a Vienna based international data centre will provide states with free expert technical analysis of IMS and other relevant data that can help in ensuring compliance.

Second, Brad Smith's proposed Digital Geneva Convention calls for establishing an IAEA like international independent organisation to identify attackers behind cyber operations.[46] Third, an internationally recognized independent cyber court or arbitrage method should be created to deal with state level cyber conflicts. The court would listen to cyberattack accusations and

[45] Fahad Nabeel, "Challenges in Implementing a Digital Geneva Convention", *Centre for Strategic and Contemporary Research*, last modified October 30, 2018, https://cscr.pk/explore/themes/defense-security/digital-geneva-convention/.

[46] Ibid.

give verdicts on the basis of findings conducted by independent and qualified experts.[47]

Presently, no international mechanism exists to define the counter measures against cyber operations, or provide collective authorization for conducting cyber operations. Therefore, it is important to formulate clear cut rules as to what constitutes a cyberattack and what should be appropriate counter measures. It will not only help in punishing cyber aggressors but strengthen deterrence in the form of retaliatory measures.

Cyber domain is not only dominated by states but non-state actors have a considerable presence too. In order to obstruct the cyber operations launched by non-state actors, international law principles imply that states should exercise control over cyber infrastructure and activities conducted within its territories. In other words, a state will be held responsible for any cyber operation launched by non-state actors from its territory and the victim state will reserve the right to conduct retaliatory measures. Hence, states should implement reasonable levels of security standards for their ICT infrastructure and systems to ensure that their territories remain free from conduction of cyber activities which are directed towards other states. Repeated failure of a state to deal with the elements targeting other states can result in declaring the former as a sanctuary state, which will result in counter measures by other states subject to collective authorisation and implementation.

A review of literature on compliance with international agreements shows that access to funding and professional expertise helps facilitate states in honouring their compliance commitments. In the cyber domain, national commitments for compliance vary greatly. The compliance support needed by states in the cyber domain includes expert training and capacity building measures to improve national cyber defence systems as well as enabling national officials to cooperate with international monitors. As discussed above, several proposals have been made to establish international institutions to assist states in identifying attackers responsible for cyber operations by providing technical capabilities. Therefore, the international cyber regime should establish an

[47] Elena Chernenko, Oleg Demidov and Fyodor Lukyanov, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," *Council on Foreign Relations*, last modified February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

institution which provides states with legal, technical and financial assistance to help improve supply chain security, and prevent the proliferation of malicious code and other harmful hidden functions. In addition, the proposed institution should also assist states in investigating cyber intrusions which are originating in or routed through their territories. Failure to have such an institution will not encourage states to comply with the cyber regime.[48]

Conclusion

Cyberspace has emerged as the fifth domain of warfare where states are engaged in short of war battles to disrupt critical infrastructure of rival states. The rapid technological advancements have enabled smaller states to challenge large states because of their cyber capabilities. Without the formulation of an international cyber regime, the rapid weaponisation of cyberspace will have destructive consequences for several states.

Some experts believe that it is nearly impossible to establish an international cyber regime due to a number of factors like rapid technological advancements, verifiability problem, etc. Contrarily, various experts believe that weaponisation of the cyber domain can be contained through effective arms control in the same way as several international arms control treaties or agreements have been doing since the 20th century.

For more than a decade, a number of initiatives have been launched for development of norms and the applicability of international law to the cyber domain. Although no considerable breakthroughs have been achieved, the initiatives have played a substantial role in formulating a blueprint which will be the basis for an international cyber regime.

An analysis of the approaches of the US, China and Russia towards an international cyber regime reveals that the great powers are leading two main camps. The US is leading the bloc which propagates an open internet whereas China and Russia are dominating the bloc which stresses the importance of sovereign control. Despite their differences, the three countries identify various common threats like the use of ICT for terrorism and cybercrimes. The three

[48] Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy & Technology 31,* no. 3, (2018): 397.

cyber advanced countries need to play an important role towards the establishment of an international cyber regime by basing their cooperation on identified common threats. For example, both China and the US reached an agreement to deal with cyber espionage for commercial purposes. Similarly, the US and Russia should conclude a realistic agreement, limited in scope. Materialisation of an international cyber regime is a long and complex journey. The US should shun the belief that by accepting binding international rules it will constrain its own hands. China and Russia have almost equal cyber capabilities as compared to the US. The American leaders need to approach the issue with the same foresight which their predecessors showed in the 1950s and the 1960s when dealing with the global nuclear arms race.