Introduction

The emergence and growth of the internet characterized by ranging innovations in all fields have positively impacted human life. The widespread use has made the world more reliant on it than before, but the risk of cyber-attacks comes with this convenience. This rising risk arises the calls for cyber security. Cybersecurity is the process of protecting and enhancing computer systems, networks, devices and programs from any cyber-attacks. The post-pandemic era, current working environment, and the recent cyberattacks and spyware controversy call for urgent attention and cooperation in the cyber domain. The lack of initiative and minimum cooperation poses countless security challenges to the world. The 2017 Black Hat Europe Attendee Survey also predicts that the next major global threat could be the weaponizing of ICT's to devastate critical infrastructure or military logistics networks by state or non-state actors.

The weaponizing of ICT's will likely upsurge the asymmetric warfare and offensive dominance conflicts between countries or groups with cyber capabilities. However, it could drag countries into the arms race and even hot wars due to the emerging role of cyber tools in military operations. As a result, cyberspace will likely accumulate and concentrate in the military and intelligence gathering field, despite encompassing far more areas. This situation and the evolving cyber domain will probably influence and transform the international field and the very security concept. The threats associated with cyberspace call for an urgent collaboration amongst all the state actors. Also, the rising multipolarity of cyberspace and the advent of post-liberal world practice makes it necessary to have an international code of cyber conduct.

Challenges in Cyber Security Cooperation

The cooperation involves multiple challenges that need to be acknowledged and addressed to find feasible solutions and create awareness of the situation in the cyberspace arena. The non-alignment of countries' solid and divergent national interests makes cyberspace's international consensus and cooperation challenging to achieve. Russia, China and Cuba's disagreement in the UNGGE negotiations during the 2017 session over the applicability of the UN Charter indicates disputes and differences in the process of cyber cooperation. This divide between the states over the varying issues of cyber sovereignty, online rights, and the conflict on making international law applicable to cyberspace or wanting a new treaty explicitly tailored to cyberspace creates a significant hurdle in achieving conventional international treaties. It causes an increasing multipolarity and the rise of the offensive strategy adopted by state and non-state actors against each other. These situations pose a

unique challenge for policymakers to address the international cyber cooperation and inherently transnational nature of cyberspace. The zero-sum game, double standards, and lack of feasible solutions in the international arena are causing us to rely on the antiquated legal regime, leaving the entire cyberspace, digital economy, and critical infrastructure exposed to cyber-attack vulnerabilities. These softer and little efforts so far have restricted the scope of more extensive cooperation.

Image source: Twitter

The Way Forward

The action should be taken that aims to maximize international cooperation and minimize politicization and cyber risk. Global efforts need a recalibration to mitigate the threat associated with cyberspace. The new form of cyber-space and security development should stress the core idea of win-win cooperation. International cooperation should advocate the basic principle of peace, shared governance and shared benefits in international exchange and collaboration in cyberspace. There should be an urge to work on the universal convention based on existing alternative proposals.

International efforts like the Budapest Convention and Russia-led Resolution should amplify at a much higher level of cooperation. The members of both the international accords should consider working inclusively together to have a global engagement strategy on cybercrime. The Budapest Convention is a framework for international cooperation against cybercrime, as it is a binding international instrument that provides guidelines for countries developing comprehensive action through legislation against cybercrime. Also, the Russian-led resolution involves the same cyber field, focusing on countering the use of information and communications technologies for criminal purposes by enhancing coordination and cooperation among states. It should apply the multi-stakeholders approach like the governments, global industry, academia, cybercrime experts and civil society to resolve the difference, prevent cyberwar and mitigate the risk of offensive cyberattacks. The upcoming Octopus Conference 2021 provides an opportunity for all multi-stakeholders to use the virtual platforms to propose innovative and feasible changes to the existing international cyber laws, as it also marks the 20th anniversary of the Budapest Convention. The Council of Europe holds the conference in cooperation with the Hungarian Chairmanship of the Committee of Ministers. The platform will help initiate and develop solutions to existing international cyber laws and failed negotiations to reach a global consensus at international institutions. The institutional mechanism of the United Nations on the open-ended intergovernmental expert group on cybercrime is already in place for global cooperation to tackle cybercrime. It will lead to adopting a much liberal approach to fight the dangerous effects of anarchy in cyberspace.

Image source: Council of Europe

The upswing of the initiatives at the global institutional level will facilitate the domino effect by setting up a chain for producing space in the cyber diplomacy field. Diplomacy has always played a crucial role in shaping peace and tranquillity in the international arena, and it has always helped to create a mindset of cooperation. The cyber-attacks are frequently transnational in response, so to retort to cross-national cyber-attacks, collaboration is required in information sharing, evidence collection, and criminal prosecution" of attack perpetrators. So here, the role of cyber diplomacy comes into play, acting as a facilitator and deterrence to such cyberattacks with cooperation and coordination. It will help mediate at a much higher degree and simultaneously reduce the uncertainty through increased information. The cyber-diplomacy transition to the post-liberal world practice due to the increasing multipolarity in cyberspace will offer a platform to those that did not have a say in the making of cyberspace structure. It will help in the making of an international society in the digital age. This will make the global cyber institutions, involved parties, and observers maintain checks and balances on the active actors in the diplomatic process. The U.S and China agreement can act as a power of example for cyber diplomacy, as the reports indicate a significant reduction in commercial espionage by Chinese sources since 2015. So the cyber-diplomacy is not only necessary but an opportunity to open other prospects of cooperation in climate change, public health, and international human rights. So the cyber-

diplomacy can create a global consensus and collaboration to reach a common ground to solve the problems associated with cyber security cooperation.

The major superpower countries should cooperate to demarcate responsible behaviour in the cyber arena. The front-runner countries involving the U.S, Russia, China, European Union, etc., having high-end cyber technology with significant offensive and defence capabilities, need to start a dialogue. The involved countries should formulate rules to avoid monopolizing the ambitious projects promoting cyber tech companies emerging from a specific country. They should focus on making cyber laws intertwined and integrated so strong that they will hold each other accountable for any malicious activity. It will restrict cyber autonomous weaponizing at the global level. The GGE meeting on lethal autonomous weapon systems is an excellent venue for concrete steps and strengthening a code of conduct. This type of arrangement will at least reduce the state-sponsored attacks.

Apart from the global efforts, there is a need to promote international cyber laws, build resilient cyberspace and eliminate the digital divide at the regional level to address common cyber threats with the help of regional organizations like ASEAN, Shanghai Cooperation and BRICS.

Conclusion

The progress in cyber collaboration will come from agreed rules, harmony and unity. It will help shape a new order and build bridges of trust and tranquillity between different political visions in cyberspace, creating a stable global digital economy. The world should start incorporating the changes based on international cooperation to fill the problem of policy vacuum and not wait for a major cyber-attack to make the cyber-space safer and protected.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments