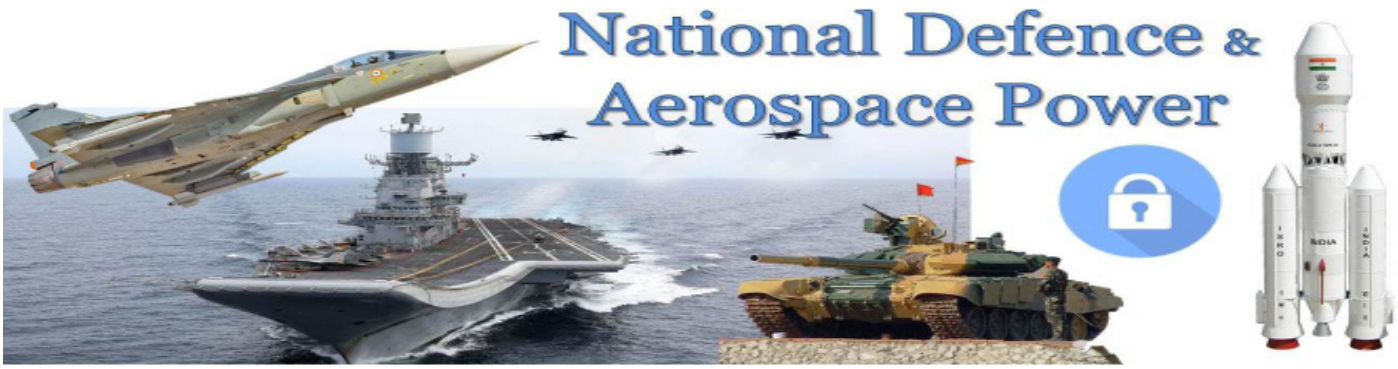
Centre for Air Power Studies



Centre for Air Power Studies ISSUE BRIEF

180/22

19 July 2022

CYBER PERSISTENT: A GAME CHANGER FOR NEW AGE NORMS

Khyati Singh

Reseasrch Associate, Centre for Air Power Studies

Norm creation, as easy as it may sound, has been a rather difficult process to initiate on a global level. Especially when cyberspace is concerned. The cyber laws that are in place don't address the issues that cyberspace deals with. Hence, apart from introducing a set of laws, it is equally crucial to have in place norms that are appreciated and acknowledged by the stakeholders alike. Moreover, much like field warfare, which runs on a combination of norms and practises that the players consider as given, cyberspace too runs on a similar understanding. However, the norms for cyberspace are not clearly defined and, at large, lack the rigour to hold the actors accountable. The forerunner of this norm creation has been the United Nations Group of Government Experts (UNGGE) and Open-Ended Working Group (OEWG) where they have argued for certain deliberative norms and agreements that can bring the member states of the United Nations into the fold of international law on cybersecurity.

The norms for cyberspace are not clearly defined and, at large, lack the rigour to hold the actors accountable.

The point at issue, however, is the nature of these norms. The norms that the groups have pitched fall short of the desired strength that is required to control cyberspace. Traditional models and mandates of forming prescriptive norms that instil regulatory behaviour amongst the states will not be able to tame the menace created in and by cyberspace. The states involved in the process of developing these laws have been rather sluggish in their approach, which in turn has been been cost heavy for them.[1] Global Commission on the Stability of Cyberspace (GCSC), which is a multi-stakeholder organization for internet governance, put forth a series of prohibitive norms that can help tone down cyberspace atrocities. Moreover, the international community needs to pull themselves together to engage in dialogues that lay down a roadmap for the same.

The norms that are proposed by the UNGGE and OEWG are not binding in nature. The nature of these norms is largely prescriptive and rarely prohibitory. In addition, even the prohibitions that it has laid down are non-justiciable, which thus makes cyberspace security laws a mere set of guidelines. There are eleven norms that have been brought to light in total, only two of which are prohibitive in essence. The others chart out duties or precautions that states should take to protect their cyberspace. These include sharing technology to help fellow countries deal with cybercrime, extending support, and protecting critical infrastructure and supply chains from cyberattacks on various grounds.[2] The two prohibitory norms direct states to not support or conduct any attack that affects the critical infrastructure of other states, and to not get involved in harming the information system of another state or the international community at large. The biggest drawback of these norms remains their uninformed approach toward the nature and behaviour of both state and cyberattacks. Most states are directly involved in cyberattacks, nor are they after critical infrastructure in the normal course of action. The cyberattacks don't happen in a blink of an eye at the level of states. Rather, they are planned, steady, and consistent penetrations that affect a system on so many levels and work until they are caught one day, or till they bring the entire state system down.

Global Commission on the Stability of Cyberspace (GCSC), which is a multi-stakeholder organization for internet governance, put forth a series of prohibitive norms that can help tone down cyberspace atrocities. Moreover, the international community needs to pull themselves together to engage in dialogues that lay down a roadmap for the same.

Cyber Norms Proposed by the Global Commission on the Stability of Cyberspace

The norms proposed by GCSC in their reports are far more detailed and cater to the real problem.[3] Instead of addressing the issues in an abstract manner, they have taken into account the real nature of cybercrime and how it affects a state's ecosystem. For instance, the GCSC explicitly mentions that both state and non-state actors must refrain from being involved in any technical affairs that might disrupt or tamper with any critical infrastructure that is essential to keep the sovereignty of a state intact. This may include their election process, referendum, policy-making, etc. Moreover, there should not be any tampering with products or services that are meant for export and can cause an conflict in cyberspace. These norms have been shaped by the attacks that have taken place in the past that caused disruption in the state machinery. Therefore, they are much more credible and practical.

In addition, GCSC reports have constantly highlighted the importance of and threat to the critical infrastructure that has increasingly become a cause of worry amongst all the nations alike. These attacks are directly related to the strategic concerns of a country and expose them to the direct wrath of their enemy. For example, in 2016, the reports of the U.S. Senate Select Committee mentioned how there had been an unprecedented level of involvement by Russia in the state elections.[4] The report claimed that there were a series of cyberattacks that tried to change the voter data or delete it altogether for states like Illinois and Arizona. This attack on the home of a great power sent a clear message across that wars were no longer traditional in nature. This wake-up call to the world was timely received by many nations, including the Dutch government, which feared cyberattacks from advanced persistent threat (APT) groups in Russia and hence opted for the manual tally of votes.[5] Therefore, it is important to dump the usual ways of norm-making by the UN and actively look for laws that states can adhere to effectively.

The U.S. tried to prevent its adversary Russia conducting cyberattacks by economic sanctions, but they still couldn't get everything in place. This is largely because cybersecurity can't be performed in isolation.

Creating "Conformance Culture"

Since there are no strictly designed and followed laws on cybersecurity that are in place, the onus shifts on all the states alike to cultivate a conformance culture that abides by the norms proposed by the UNGGE, OEWG and GCSC commissions. The lead by norms implies that entrepreneurs have to be shouldered by states to help bring stability and security to cyberspace. So far, the states have not excelled in any norm manifesting culture, and this puts the culprits at an advantage as it allows them a larger space to manoeuvre without any consequence.

To bring state behaviour to such a level of conformance would require dedicated and collective efforts. So far, states like the U.S. tried to prevent its adversary Russia conducting cyberattacks by economic sanctions, but they still couldn't get everything in place.[6] This is largely because cybersecurity can't be per-formed in isolation The entire ecosystem has to be made available to ensure that cyberspace is secured. Unless everybody is safe, everybody is unsafe in cyberspace, this is the standard modus operandi. Economic sanctions are increasingly being waived through the use of cryptocurrency, and tracking them down is becoming equally difficult due to the integrated cyber exploitation. Hence, all the leakages need to be fixed to get the system functioning at ease.

An interesting approach has been the development of cyber persistence.[7] This accounts for both state and non-state actors working together to constrain actors that don't abide by the prescribed norms. For instance, actively exploiting a vulnerability and learning its pattern, then closing it down along with shutting all the ways of its

re-instalment and with bringing all the practices and indicators used by it into the public domain. This theory of cyber persistence insists on persistence in place of coercion. Persistence works as a trap which allows the vulnerabilities to consider that the security setup allows them to penetrate, and this tactic of bargaining helps the state gain an edge over their adversary. The fact that this approach allows for both government and private actors to play a role together makes it functional across all the stakeholders. Since a majority of service providers for these critical infrastructures are rooted in private firms along with having a dense network base amongst the citizens, hence, their collaborative norm acceptance would yield the desired change in the security setup.

Despite certain acts in place, the larger argument of initiating a cyber-persistence norm that paves the way for larger conformance to prohibitive norms is missing in India at large. The staff at cyber cells are often overburdened due to the lack of decentralization at the system level.

The US Department of Defense implemented a similar approach that is often called the 'defend forward cyber strategy' which is operationalized by the U.S. Cyber Command's (CYBERCOM) doctrine of "persistent engagement."[8] This doctrine incorporates measures for achieving security through persistent exploitation-based operations, responsible use, and campaigns. The CYBERCOM mostly aims at dealing with the cyberattack at the threat source. One of CYBERCOM's operations brought down the world's largest botnet, namely Trickbot. This was done to remove the possibility of any disruption in the U.S. elections in 2020 after the lessons it learnt from the previous incidents that pointed to tampering with elections by Russia. States at large can pursue this mechanism, which will help introduce the conformance that is needed to deal with the technical infrastructure challenges as has been suggested by GCSC.

However, the actors involved to secure cyberspace need to constantly keep in mind the fact that an adversary that has been taken down by the state or non-state actors will quickly reconstitute its offensive capabilities. The teach-war in cyberspace is a vicious cycle where technology outpaces technology at every level. The CYBERCOM operation at Trickbot was ruled out by them in no less than two months, and they were back in place with better capabilities to counter any such strike.[9] Hence, the immediate security assurance that these operations give needs to be made perpetually available by expanding and extending them into cyber persistent campaigns that allow for a culture of conformance against the prohibitive norm of botnets to grow.

The government alone doesn't benefit from conforming to the prohibitive norms. The private industries have incentives to follow a similar trajectory. Furthermore, many industries, over a period of time, have developed their capabilities to an extent that allows them to be involved in responsible exploitation-based operations. Giant tech ventures like Microsoft include prohibitive norms in their company policy as expressed in their

Digital Geneva Convention paper.[10] It has a Digital Crimes Unit that is meant to secure cyberspace and exploits legal and technical capabilities to recognize, investigate, and derange malware that facilitated any kind of cybercrime or caused disruption in regular practices. In addition, Microsoft has also extended a helping hand to the FBI to coordinate attacks on various botnets like ZeroAccess and Citadel. These joint operations flag the possibility of the private sector and the government coming together to safeguard cyberspace.[11]

At present, the larger cyberspace in India is being operated on more abstract terms where the dissemination of information and awareness is still weak amongst the masses, and hence they end up being the easy prey of attackers.

Cyber Laws in India and the Road Ahead

Cybercrimes in India are growing exponentially and account for the loss of nearly Rs 1.25 lakh crore annually. The reports suggest that there were nearly 3.3 million cases in just the first quarter of 2020. These attacks are bound to grow if we don't put in place stringent laws that address the problem at all levels. Currently, there are four major cyber laws in India that deal with cybercrime at all levels.

The Information Technology Act 2000 is a 22-year-old law and was initially meant for inclusiveness in eCommerce, but over time it has had a series of amendments and includes sections that deal with computer-based fraud, receiving stolen computers or devices, damaging the computer system of another person, etc. The Indian Penal Code (IPC) 1980 broadly covers cyber frauds under various sections and has included in its fold crimes like reputation damage, false documentation, forgery, etc. Thereafter, the Companies Act of 2013 brings into the picture the legal obligation a company has to cement all the technical and legal aspects and ensure cybersecurity. Lastly, the National Institute of Standard and Technology (NIST) compliance, which was authorized by the Cybersecurity Framework to put in place an approach to cybersecurity that is globally certified. The NIST Cybersecurity framework engulfs all the guidelines, practices, and standards to deal with cyber risks in an efficient manner.[12]

However, despite certain acts in place, the larger argument of initiating a cyber-persistence norm that paves the way for larger conformance to prohibitive norms is missing in India at large. The staff at cyber cells are often overburdened due to the lack of decentralization at the system level. Moreover, India doesn't have cyber courts in place that can quickly track down the attacker and bring him to justice. Speed and time are essential components of cyberspace and any slackening on those front costs the entire operation a heavy sum. Therefore, for a country as vast and as openly integrated into the global networks, it is important to bring in drastic policy changes at all levels and inculcate the suggestive norms of GCSC in the discourse. Furthermore, the government needs to bridge the digital divide that is operational between the government sector and

the private players. Much like the U.S., India too can bring big industries into the loop and can exploit their advanced tech capabilities to strike down cyberattacks before they wreak havoc on the system.

At present, the larger cyberspace in India is being operated on more abstract terms where the dissemination of information and awareness is still weak amongst the masses, and hence they end up being the easy prey of attackers. A good initiative in this direction would be to store the personal information of the citizens in India only, as has been the case with the United States under Health Insurance Portability and Accountability Act 1996 (HIPAA) compliance, which charts out the lawful use and dissemination of protected health data.

To conclude, India needs to introduce a cyber-friendly culture that doesn't operate from the top level alone but is equally functional at the grass root level because in the cyber ecosystem, everybody connected to the internet is a stakeholder and is equally, if not more, exposed to the threat that sits in the cyberspace domain. Hence, the chain connection needs to be kept in mind while formulating laws and introducing norms.

Notes:

[1] Joseph S. Nye, Jr, "The End of Cyber Anarchy?", *Foreign Affairs*, January 2022, https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy. Accessed on July 1, 2022.

[2] "Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law", UNGGE Report, 2015, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/. Accessed on July 1, 2022.

[3] "Advancing Cyber stability", Global Commission on the Stability of Cyberspace, GCSC Report, November 2019. https://cyberstability.org/report/. Accessed on July 2, 2022.

[4] Dana Farrington, "Senate Intelligence Report on Russian Interference in The 2016 Election", *NPR*, July 2019, https://www.npr.org/2019/07/25/745351734/read-senate-intelligence-report-on-russian-interference-in-the-2016-election. Accessed on JULY 2, 2022.

[5] Erik Brattberg, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks", Carnegie, May 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435. Accessed on July 1, 2022.

[6] Michael Fischerkeller, "Initiative Persistence as the Central Approach for US Cyber Strategy", Kyberno, July 2021, https://www.artsci.uc.edu/content/dam/refresh/artsandsciences-62/departments/political-science/ccsp/pdf_downloadableflyers/Kybernao_PaperSeries_Issue1_Final.pdf. Accessed on July2, 2022.

[7] Paul Nakasone, "How to Compete in Cyberspace", *Foreign Affairs,* August 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity. Accessed on July 2, 2022.

[8] Department of Defense, "Cyber Strategy 2018", https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. Accessed on July 2, 2022.

[9] Liviu Arsene, "TrickBot is Dead. Long Live TrickBot!", Bitdefender, November 2020, https://www.bitdefender.com/blog/labs/trickbot-is-dead-long-live-trickbot/. Accessed on July 2, 2022.

[10] Microsoft Policy Papers, "A Digital Geneva Convention to protect cyberspace", https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH, Accessed on July 3, 2022.

11 Joseph Demarest, "Taking Down Botnets", FBI, July 2014, https://www.fbi.gov/news/testimony/taking-down-botnets. Accessed on July3, 2022.

12 Cybersecurity Laws in India, "Everything About Cyber Security Law & Regulations in India", Appknox, https://www.appknox.com/blog/cybersecurity-laws-in-india. Accessed on July 3, 2022.

Centre for Air Power Studies

The Centre for Air Power Studies (CAPS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Marshal Anil Chopra PVSM AVSM VM VSM (Retd).

Centre for Air Power Studies
P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Dr Shalini Chawla e-mail: shaluchawla@yahoo.com
Formatting and Assistance: Ms Mahima Duggal, Mr Mohit Sharma and Mr Rohit Singh