Submission of Comments to the GCSC definition of ‘Stability of cyberspace’

Arindrajit Basu and Elonnai Hickok
Centre for Internet and Society, India
September 6th 2019

Survey Information (Civil Society - Academia)

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa.

We thank the Commission for the opportunity to provide comments to the definition of ‘stability of cyberspace’ and associated explanation. We hope that the feedback provided can work to strengthen the definition and ensure that it can be used as an effective policy lever that ultimately strengthens the security and rights of the individual and as a tool to bridge gaps between stakeholder groups.

Introduction

Security should therefore be considered a positive concept - a state of feeling secure rather than the mere absence of harm.[1] We thank the GCSC for arriving at a definition that recognizes the user’s perception as a point of entry rather than focussing on parameters drawn up by the state as the concept of national security or interest can be weaponized by states to set an agenda as well as restrict user’s access, availability and rights in cyberspace.

At the same time, we find that the use of certain redundant terms; a reduction of scope and a lack of detail in the explanation hampers this admirable vision. We hope our comments are helpful in bridging some of these gaps and add to the quality of what is already set to be a seminal definition.

[1] Anja Kovacs and Dixie Hawtin, “Cyber Security,Cyber Surveillance and Online Human Rights” *Stolkholm Internet Forum*, 2013, at <https://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf>

Targeted Comments Wording

'Condition': It is unclear that stability in cyberspace should be conveyed as a 'condition' that is sought to be achieved. Stability in physics can be understood as a physical state where externally induced displacements catalyze changes that balance this displacement returning the body back to its original state of equilibrium. Stability as a condition of security is difficult to define as there are various parts including network dynamics and topology, technology disparities etc. This leads to the creation of a goal that is difficult for policy makers to translate into effective policy. *We recommend borrowing from language around stable governance*[2] *and replacing the term 'condition' with the phrase 'objective' -which can allow policy makers to develop policy towards a defined outcome so it will read "...Stability of cyberspace is the objective where ..."*

'Reasonably confident': We feel that the use of the word 'reasonably' is redundant and dilutes the robustness of the definition. The definition of 'reasonably' in this case is to "a moderate or acceptable degree." Yet it is unclear from which perspective 'reasonably' will be understood - from the state, the corporate, or the individual? The point of this definition is to arrive at a threshold of stability that is acceptable to all users. As the explanation suggests, that the very essence of cyberspace hinges on a perception of its stability - a perception that the dilution in this phrase directly contradicts.

If user confidence is an objective of this definition, we see no additional value that the use of the word brings to this sentence and recommend deletion of the term 'reasonably.'

'Confident in their ability to use cyberspace safely and securely': We feel that the focus of this phrase on the 'ability' of the individual to use cyberspace shifts the burden away from state and large private actors who develop, control, modulate access to and otherwise play a role in regulating cyberspace and incorrectly places it on the 'ability of the individual' to use cyberspace safely and securely. In effect this conflates two separate policy issues-first, the need to skill and build capacity among individuals and communities that use the digital space and second, the safety and security that powerful actors should endeavour to provide. Confidence in one's ability is an entirely different question from confidence in the stability of an externally modulated phenomenon like cyberspace. Also, the confidence in the ability to use cyberspace safely and securely hinges on many aspects including education, availability of appropriate user interfaces, cost of access, technological complexity, etc. Defining which areas can be addressed to increase confidence could be useful for policymakers.

Therefore we recommend changing the phrase to 'confident in the safety and security of cyberspace'-which highlights and places the emphasis on the stability of cyberspace.'

[2] For example, the United States Institute of Peace has defined stable governance as "an end state where the state provides essential services and serves as a responsible steward of state resources government officials are held accountable through political and legal processes; and the population can participate in governance through civil society organizations, an independent media, and political parties." For more information see: https://www.usip.org/guiding-principles-stabilization-and-reconstruction-the-web-version/stable-governance

‘Generally assured’: Like the use of the word’ reasonably’ in Point 2, the use of the word ‘generally’ is a redundant dilution-which causes the definition to lack teeth. We agree that the obligation to ‘assure’ the integrity of services may be too high a burden as new forms of attack vectors continue to proliferate and defense mechanisms rush to keep up.

Therefore, in line with the explanation that stresses on the importance of perception, we recommend changing the phrase to “can be relied upon”. The new wording indicates that there is no need to provide a guarantee in the safety and security of cyberspace but enough of certainty to indicate that an individual using cyberspace can rely upon it.

‘Relative peace’: We feel that the use of this phrase is redundant. Managing change in ‘relative’ peace beckons the question of what the peace is being considered in relation to. Like, the other redundant prefixes addressed above, we feel that the use of the word ‘relative in this case dilutes the notion of peace unnecessarily. We also believe that the word ‘peacefully’ is amorphous with no explanation or reference parameters. As the objective of International Law and the UN Charter is an universal instrument that seeks to promote peace and stability in global affairs, reference to the tenets of International Law and the UN Charter might help clarify the term ‘peaceful,’

We therefore recommend deleting the term ‘relative peace’ and replacing the phrase to “ where change is managed and tensions resolved in a peaceful manner in line with the principles of International Law and the UN Charter.”

Scope

We feel that the exclusion of some key concepts from the definition dilutes its efficacy and makes it irrelevant in certain global contexts. We identify some of these gaps and make recommendations for additions below:

Incorporating Communities and groups: Presently, the definition identifies individuals and institutions as the stakeholders to whom a stable cyberspace should be available to. Given the interconnected and networked dynamic of cyberspace, where technology can impact groups of people and given the use of cyberspace by individuals that identify by groups and communities, there is growing recognition that there is a need to recognize the ‘individual’ in cyber space in a more nuanced manner through the recognition of communities. We see this reflected in emerging policy - for example India is presently proposing a category of ‘community data’ that is owned by the community and treated differently from personal data.[3]

The notion of ‘community data’ appears both in the Srikrishna report that accompanied the draft Data Protection Bill 2018 and the draft e-commerce policy. However, there appears to be some conflict between its usage in the two policies. When defining community data, the Srikrishna Report endorses a collective protection of privacy by protecting an identifiable community that has contributed to community data. The draft e-commerce policy appropriates the notion of community data and re-conceptualizes it instead as ‘societal commons’ or a

[3] See https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

'national resource' whereby the community has rights to access such data but the government has ultimate and overriding control of the data. While there are concerns with this definition that we have raised previously, it is still important to recognize that the community becomes an important point of departure in this instance.

In its *Digital Economy Report* 2019,United Nations Conference on Trade & Development (UNCTAD)[4] has also recognized the concept of 'community data.' Their report acknowledges that some data such as traffic data from a ride sharing application should be termed as a public good and shared with the public authorities to assist with the management of traffic. However, the public data could also be abused and in the words of the Report, the "*necessary and inalienable embeddedness in the relevant group/community strengthens the case for close community access, control and rights over its data, and of the digital intelligence that can be derived from that data*." A direct consequence of that is that a community centric perception of stability must be considered in order to provide an all-encompassing definition of cyber stability

We believe that incorporating communities and groups would also in turn translate into a more culturally nuanced conceptualization of "stability" that can speak to multiple values-including the need to reconcile development goals in cyberspace with security concerns. Cyber stability is certainly concerned with security of systems from external actors but it is equally concerned with the mending of power dynamics between those who engage with and use the space. Due to the extractive economic models[5] floated by tech companies, largely based in the Global North, several communities largely situated in the Global South alienated from the incoming digital dividend and do not feel directly the benefits of cyber stability as they are not sure how their data might be exploited. Recognising groups and communities as an entry point in the definition allows for the bridging of this divide as it recognizes that cyberspace can be conceptualised as a vehicle for empowering specific communities. Furthermore, Human Rights law often looks at protecting individuals through the protection of communities and groups such as women, children, migrants, minorities, and indigenous peoples.[6]

We thus recommend that the definition be amended to identify "individuals, communities, groups and institutions".

Including Access: Presently, the definition relies on availability and integrity as the two defining indicators for services in a stable cyberspace. Though important, we are concerned that using only availability and integrity as indicators limits the discussion to infrastructure and could legitimize trends that we have seen such as network shutdowns, censorship, and restriction of access to online services. It could further allow governments to claim to support a stable cyberspace while undermining access to the same. Including language around 'access' can also help to bridge efforts around stability of cyber security and efforts around bridging the digital divide.

[4] " Digital Economy Report 2019: Value Creation and Capture for Developing Countries" (2019) https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

[5] https://www.nytimes.com/2019/01/18/books/review/shoshana-zuboff-age-of-surveillance-capitalism.html

[6] See: https://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html

We thus recommend that the definition incorporate 'accessibility' as a third defining indicators for services in a stable cyberspace.

Recognizing the spectrum of 'tensions': Presently, the definition captures various forms of geo-political disagreements and challenges in cyberspace as 'tensions'. We feel it is important to capture in a more nuanced way the spectrum of geopolitical tensions that exist in cyberspace to establish the scope of what needs to be considered when working towards a stable cyberspace.This could include 'below the threshold' operations such as information espionage or the spreading of misinformation and disinformation;and full blown cyber conflict that would cross the threshold of use of force as per Article 2(4) of the UN Charter.Using the example of shutdowns, we would hope to protect against a government claiming to support a stable cyber space while enforcing network shutdowns for internal political reasons.

We would recommend that the definition expand upon this word and illustrate it by Including the phrase " tensions ranging from external interference in sovereign processes to the use of force in cyberspace."

Explicitly referencing rights: Presently the definition relies upon 'safely and securely' as the indicators for use of a stable cyber space. Not linking the definition to rights does a great disservice to the original vision of this definition which lies in a user-centric reliance on the stability of cyberspace. Clearly recognising user rights furthers this notion and ferments the alignment of practice and policy in cyberspace to international human rights standards

It also allows for cyber security to clearly be linked to individual security and moves beyond the artificial measurement of the security of infrastructure by the government that then in turn decides the security of societies. Often, actions by governments such as unjustified internet shutdowns or unbridled surveillance measures are -justified by the 'trump card of national security[7] and legitimized by law and policy that ends up furthering instability in cyberspace.Therefore, explicitly recognizing rights creates credibility and certainty in the stability of cyberspace and should form an important part of this definition.

Drawing from the explanation, we would recommend that 'rights respecting' is brought in as a third indicator for use of a stable cyber space.

Addressing Accountability and Stakeholders: The definition currently does not identify specific actors in cyber space nor does it speak to the role that accountability of each stakeholder plays in maintaining cyber stability. We suggest that the threshold of accountability should be devised against the exercise of an obligation of due diligence.by all stakeholders that impact,modulate and potentially restrict the accessibility, availability and integrity of cyberspace for others.The International Court of Justice has stated that due diligence is an obligation of conduct and not of result.[8] The due diligence standard should be

[7] Jennifer A. Chandler, "Personal Privacy versus National Security: Clarifying and Reframing the Trade-off" in Orin Kerr, Carole Lucock and Valerie Steeves, eds. *On the Identity Trail: Anonymity, **Privacy** and Identity in a Networked Society*, (Oxford Univ. Press, 2009) 121,122

[8] J.G. Lammers,Pollution of International Water Courses A Search for Substantive Rules and Principles 524 (1984)

evaluated on a two-pronged test - of knowledge and capacity.[9]While traditionally applied to states, the definition should also impose the similar obligation on private actors operating in this space.

We recommend adding an additional line in the definition which states that " Cyber stability can only be fostered if key stakeholders in cyberspace conform to a due diligence obligation of not undertaking and preventing actions that may prevent cyber stability."

Explicit restraints on offensive action: Instability in cyberspace is aggravated by the uncertainty cultivated by the dual-use nature of cyber grids. Common place components of the Internet of Things (IoT) such as refrigerators can be repurposed and data repositories of health data, personnel data, or financial records can be infiltrated as part of offensive cyber strategies. While it may not be possible to effectively outlaw all cyber operations, it is possible to create legal rules that place restraints on the methods and intended impacts of these operations.

With the cyber norms process in a state of development, there is a great deal of legal uncertainty that is furthering instability in cyberspace.Any useful conception of strategic stability must, then, seek to minimize or eliminate immaterial or peripheral incen-tives to using offensive cyber strategies-first, while preserving and potentially legitimizing incentives that enable offensive cyber operations in a manner that can further effective deterrence and thereby foster stability, while also minimising any collateral damage to civilian life or property.[10] This framework must indicate 'red lines' on the illegitimate effects and intents of cyber operations but also chart out scenarios in which offensive cyber operations may be legitimate.[11]

We recommend adding an extra line which states that " The end goal of cyber stability must minimize or eliminate immaterial or peripheral incentives while preserving and potentially legitimizing those cyber offensive operations that can further effective deterrence and thereby foster stability, while also minimising any collateral damage to civilian life or property."

New Definition

Amalgamating our suggestions above, below is the new definition of cyberspace that we place before the Commission for their consideration:

Stability of cyberspace is the **objective** where individuals, institutions **and communities** are ***confident*** *in the safety and security of cyberspace; the* **accessibility**,availability and integrity of services in cyberspace **can be relied upon and** where change is managed and tensions *from external interference in sovereign processes to the use of force in cyberspace* are resolved peacefully in line **with the tenets of International Law,specifically the principles of the UN Charter and universally recognised human rights.**

[9] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn.& Herz.v. Serb & Mont.) [2007] ICJ 2 (Feb. 26) ¶ 430.

[10] https://publications.armywarcollege.edu/pubs/2216.pdf

[11] Ibid

Cyber stability can only be fostered if key stakeholders in cyberspace conform to a due diligence obligation of not undertaking and preventing actions that may prevent cyber stability. The end goal of cyber stability must minimize or eliminate immaterial or peripheral incentives while preserving and potentially legitimizing those cyber offensive operations that can further effective deterrence and thereby foster stability, while also minimising any collateral damage to civilian life or property.

Explanation

Conceptualization of Cyber Space: It is unclear from the explanation how the Commission is conceptualizing cyberspace. The security community uses the term cyberspace whereas the free speech/human rights community uses the term internet or digital. [12]Though often working towards similar objectives and in intersecting areas, these two communities do not necessarily work with each other. In an attempt to bridge policy areas with those working in digital rights we would recommend that the explanation recognize that cyberspace encompasses the internet and the digital more broadly.

Explanation of vectors and stakeholders in a 'changing cyberspace':We agree with and appreciate the paragraphs in the explanation that highlights that non-cyber political issues, policy decisions pertaining to issues around cyberspace, emerging uses of existing and new technology, and attacks on a range of aspects of cyberspace beyond infrastructure. Though the explanation clarifies that cyberspace is a domain of constant change, it can be useful for the explanation to further identify (1) factors that drive change in cyber space-political,societal,economic and technical,(2) Stakeholders that drive change,-state actors, private corporations and civil society, (3) How change impacts various stakeholders,including specific focus on marginalised communities and (4) What change management efforts could include.

As Lucas Kello has authoritatively demonstrated in The Virtual Weapon[13],cyberspace has uprooted conventional models of thinking on the International System, which recognize states as the protagonists in a global 'ordering system'[14] with 'constitutional normative principles.'[15] He identifies three orders of cyber-revolution. Third-order revolution or systemic disruption results in drastic changes within the confines of the existing state structure.[16] The drastic changes happen in both the material ingredients of power which are, in this case, defined by (1) A change in the physical architecture that defines power at the international level and (2) A change in the norms and rules which govern interactions between states. He then identifies second-order cyber revolution, which is brought about when a state or a group of states reject the shared purpose of the existing units, (systems revision) which may be exemplified by North Korea's weaponization of cyberspace.[17] Finally, first-order cyber revolution sees a change in the relative arrangement of building blocks of the international system which has

[12] Said by a speaker at the Convening of the Hewlett Foundation San Diego, 2019

[13] Lucas Kello *The Virtual Weapon and International order*, (YUP 2017) 82 [hereinafter The Virtual Weapon].

[14] Kenneth Waltz, *Theory of International Politics* (New York,McGraw-Hill,1979) For Wlt, the organising principle is the absence of centralised government, therefore leaving sovereign states as the supreme organising units.

[15] Hedley Bull, *The Anarchical Society: A study of Order in World Politics* (London, Macmillan, 1995),67-68.

[16] The Virtual Weapon, *(supra)* at 86.

[17] *Ibid*, at 90.

resulted due to the increased proliferation of non-state actors in the cyber arena. [18](systems change)

The explanation should recognise that each of these orders of cyber revolution come with different change management and mitigation techniques to clarify what the abstract idea of 'change' actually means for policy-makers and others attempting to engage with the ecosystem.

Examples

Internet shutdowns (cyber instability): such as the present one prevailing in the Indian state of Jammu&Kashmir[19] is a prime way of fostering cyber instability as it restricts the accessibility of an entire community of individuals to the internet and blocks potential communication. Unless used as an exceptional measure with strict adherence to the principles of necessity and proportionality, as well as transparency and accountability, such shutdowns are a key vector of fostering instability as it prevents individuals from relying on the continued accessibility and availability in cyberspace.

Clear declarations on the applicability of International Law in Cyberspace (furthering cyber stability)

We believe that the clear articulation of the application of International Law in cyberspace helps foster stability as it positions to external stakeholders clarity broadly on how a state or non-state actor may behave in response to an offensive cyber operation or when they may engage in one. UK[20], France[21], Germany[22], Estonia[23],Cuba[24] (backed by China and Russia), and the USA[25] have all produced public statements in furtherance of this principal.

Governments exploiting vulnerabilities (potentially furthering or detracting from cyber stability): Depending on how and why governments obtain vulnerabilities and exploit the same, cyber stability could be furthered or detracted from. For example, stockpiling of vulnerabilities with no oversight or accountability for use of the same could detract from cyber stability. Establishing a VEP to govern the retention and use and disclosure of vulnerabilities could work to ensure that such actions further cyber stability. This is inline with the GCSC norm on the creation of vulnerability equities process.

Cyber attack through disinformation: (Promoting instability) Emerging examples have demonstrated that the use of cyber has become a geo-political tool to target democratic processes and institutions and brings in new forms of threat vectors and potentially malicious

[18] *Ibid*,at 92.
[19] Aayush Rathi&Akriti Bopanna, "Kashmir's information vacuum", The Hindu,Aug 29,2019,<https://www.thehindu.com/opinion/op-ed/kashmirs-information-vacuum/article29282096.ece>
[20] https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century
[21] https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law
[22] https://www.lawfareblog.com/germanys-position-international-law-cyberspace
[23] https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/
[24] https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf
[25]https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf

actors.[26] The spreading of disinformation therefore reduces the reliance that users place on cyberspace and therefore,is a source of instability.

Supporting Documents

[1] Lucas Kello *The Virtual Weapon and International order*, (YUP 2017)
[2] Anja Kovacs and Dixie Hawtin, “Cyber Security,Cyber Surveillance and Online Human Rights” *Stolkholm Internet Forum*, 2013, at <https://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf>
[3] Elbridge A. Colby, Michael S. Gerson, “ Strategic Stability: Contending Implications” https://publications.armywarcollege.edu/pubs/2216.pdf
[4]Digital Economy Report 2019: Value Creation and Capture for Developing Countries” (2019) https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

[26] https://hewlett.org/the-changing-landscape-of-disinformation-and-cybersecurity-threats-a-recap-from-verify-2019/