THE CENTRE FOR internet & society

Response to GCSC on request for consultation: Norm Package Singapore

January 17, 2019

By **Arindrajit Basu**, **Gurshabad Grover** and **Elonnai Hickok** with inputs from **Karan Saini**

The Centre for Internet and Society, India

Introduction

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. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and practices around internet, technology and society in India, and elsewhere.

CIS greatly appreciates the initiatives taken by the GCSC in bringing together various stakeholders to define, deliberate upon and implement norms that promote the stability of cyberspace. We further thank the GCSC for the opportunity to provide comments to the draft norms on the stability of cyberspace, and appreciate the inclusive and open-ended nature of this initiative.

CIS will be responding to all six norms in the Singapore Norms Package and also proposing two new norms which we feel address threats to the stability of cyberspace and can strengthen the existing body of norms.

High-level recommendations

We appreciate the variety of norms and the diverse set of stakeholders conceptualized by the GCSC. We feel that the norms and the background supporting these norms would benefit from clearer references to and articulation of existing rules and regulations and current examples justifying why the norm is necessary. We also feel that a variety of the research commissioned by the GCSC, to which CIS also had the privilege of contributing to, could be utilized as background for the framing and implementation of some of these norms.

While we have various recommendations that cater to the implementation and conceptualization of each individual norm, at a high level, we would make the following recommendations towards strengthening the document as a whole and ensuring it is relevant and complementing existing and past initiatives at a global level:

1. **Situating norms in existing and proposed work**: The document notes that it is meant to build upon the work done at the UN GGE. It would be useful for the document to more clearly articulate this link in the introduction, background of the norms or as an annex. While we recognize that the GCSC has been constantly engaging in dialogue with the other efforts, currently, it is unclear in certain cases which norm has evolved from an existing or already proposed norm. Similarly, it

would help to more clearly situate these norms in the context of relevant initiatives like the UN GGE and the Paris Call for Trust and Security in Cyberspace. This will answer questions such as how the proposed norms are similar or different from existing proposals, and how the objectives and processes of the proposed GCSC norms are different from existing proposals and processes. Such information will be key when bringing in support for the norms. Going forward, it is also necessary to develop thinking on how the various norms formulation processes can come together and echo the voices of stakeholders from all over the world.

2. **Qualify thresholds and parameters**: Many of the norms and backgrounds set thresholds and parameters such as "significant, reasonable, prioritize little/grave risk etc.". We would suggest providing principles that help in qualifying such terms to provide more clarity on what type of behavior and impact the norms are attempting to address.

3. **Harmonize and define terms**: Many of the norms and backgrounds use different terms for seemingly the same concept. We would recommend ensuring harmonization of terms throughout the document and providing a glossary of how these terms are understood by the GCSC. Examples of such terms include "cyber stability, ICT resources, cyber infrastructure, offensive cyber operations etc."

4. **Background to focus on thresholds and parameters**: Currently, many of the backgrounds for each norm read as justifications for the norm in narrative form. We would recommend the background for the norm also serve as an explanation and provide clarity on different thresholds and parameters through examples and principles. For example, the term 'reasonable level of diligence' is used throughout the norms package without articulating what the 'reasonable level' threshold is. We suggest the most proximate universally acceptable standard be looked at as a frame of reference. In this specific instance, the oft-cited international law threshold of 'due diligence' would have been a useful frame of reference. Going forward, the GCSC should look at working on technical parameters that would enable the application of existing thresholds such as due diligence in the context of cyber security.

5. **Grounding in international human rights norms and legality**: Many of the norms and background give examples of actions that would not fall within the scope of the norm. It should be clear that any behavior, within the scope of the norm or outside, needs to be legally backed and inline with international human rights norms. This is particularly true for norms touch on the use of civilian devices etc. Without such thresholds there is the risk of legitimizing illegal actions or actions that violate universally accepted human rights norms that have been widely recognised as being part of the corpus of international law.

6. **Incorporate a focus on civilians:** The scope of the norms currently extends to defining obligations governments and businesses. Civilians are also key

stakeholders - particularly when it comes to maintaining cyber hygiene. Where appropriate, we would recommend the role of civilians be clearly articulated in norms or in the background.

7. **Attribution processes and uniform evidentiary standards**: One of the major challenges to the effective implementation of this norm and ensuring compliance with the standards it sets is the challenge of attribution in cyberspace.[1]No technical routine can fully solve the problem of attribution in cyberspace.[2] However, without the possibility of credible attribution, it is unlikely that states and non-state actors will be sufficiently deterred to comply with the norm. Quality attribution depends not only on the effective use of skills and tools but also on a positive organisational culture, well run teams and cooperation across sectors, including among stakeholders that span multiple jurisdictions. This holistic approach to attribution can only be In this context, public communication regarding the attribution process become very important as it can foster public discourse on accountability standards and be a tool for cyber deterrence.[3] The RAND Corporation explored the nature of an international organization, which it named the Global Cyber Attribution Consortium.[4] The goal was to bring together a broad team of international experts to conduct an independent investigation into major cyber incidents for the purposes of attribution.[5] It would work with victims upon request and publish its methodologies and findings for review. The international community could then use the Consortium's findings to bolster cyber defences and institute follow-on enforcement actions to hold the perpetrators accountable.An extension of the RAND Corporation model that could be explored in further research is the possibility of it undertaking regular inspections to ensure cyber hygiene in all nations and ensure they are undertaking their due diligence obligations to prevent the use of their infrastructure for harbouring future attacks.

8. **Enforcement:** In addition to the engagement that the GCSC has already undertaken with UN mechanisms, the Paris Call and multiple private sector initiatives, we recommend the consolidation of relationships with the following cluster of bodies to ensure appropriate implementation and enforcement:
   (i) World Trade Organization: GCSC should consider mechanisms for engagement with the WTO and other regional trade agreements that might enable them to promote and incorporate defined norms in trade

[1] See Basu A (2018) " The Potential for the Normative Regulation of Cyberspace:Implications for India"<https://cis-india.org/internet-governance/blog/the-potential-for-the-normative-regulation-of-cyberspace-implications-for-india> 25-33

[2] Thomas Rid & Ben Buchanan " Attributing Cyber Attacks," Journal of Strategic Studies, 38 (2015) 1-2, 4-37

[3] See Basu A (2018) " Lessons learned from US response to cyber attacks" The Hindu Business Line <https://www.thehindubusinessline.com/opinion/lessons-from-us-response-to-cyber-attacks-ep/article25372326.ece>

[4] Davis, John S., Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern and Michael S. Chase. Stateless Attribution: Toward International Accountability in Cyberspace. Santa Monica, CA: *RAND Corporation*, (2017). At <https://www.rand.org/pubs/research_reports/RR2081.html.>

[5] See Basu A (2018) " The Potential for the Normative Regulation of Cyberspace:Implications for India"<https://cis-india.org/internet-governance/blog/the-potential-for-the-normative-regulation-of-cyberspace-implications-for-india> 33

agreements. This is crucial as the WTO is the most widely regime in international law.

(ii) Technical standards and norms: Standards and standard setting bodies at the national and global level can takes these norms into account when developing standards. Additionally, states should take steps to harmonise involvement in technical standards with these norms. Open technical standards play an important role in governing the growth and behaviour of ICT, and have facilitated the growth the Internet and web. While the norm to avoid tampering attempts to draw guidelines for states intervening in the production and development of ICT, there is a history of state entities exerting disproportionate influence over the standard development processes by either directly inserting vulnerabilities into standards' technical design, or swaying consensus in a preferred way through questionable means.[6] GCSC can encourage state and non-state actors to advance the goals of the proposed norms at standard-setting bodies, and also encourage non-state actors to participate in technical norms and bodies as well to advance these goals.[7] GCSC can harmonise these proposed norms with technical work in the same vein to increase the effectiveness of its proposals.

(iii) National Frameworks: The proposed norms can be built into national frameworks for cyber security for both critical infrastructure and cyber security more broadly.

Norm-specific recommendations

Norm to avoid tampering

"State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace."

1. Norm

The use of the phrase "if doing so may substantially impair the stability of cyberspace"a vague and unnecessary qualifier for several reasons. *First,* any tampering that impairs the stability of cyberspace, even minimally, should not be permitted *Second*, targeted

[6] *See* Aayush Rathi, Gurshabad Grover and Sunil Abraham (November 2018) "Regulating the Internet The Government of India and Standards Development at the IETF", <https://cis-india.org/internet-governance/files/regulating-the-internet> pg. 5

[7] *As the norm package points out, there are mutually agreed norms between service providers that advance routing security, see* Mutually Agreed Norms for Routing Security (MANRS), <https://www.manrs.org/>

intervention and tampering should only be permitted after the product and service is deployed: while this may increase costs of achieving the goals of combating criminal activity, it significantly reduces harm that can arise out of mistargeting of tampered services and products. *Third*, such state intervention is generally unviable without the active involvement of non-state actors, mainly private companies, that produce and develop ICT products; thus, at scale and when such activity is directed at other states, the operations in effect lead to a violation of the proposed norm against offensive cyber-operations by non-state actors. We propose the following text instead:

> **"State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with."**

2. Background Notes

- We recommend that the background note highlight the risks of tampering with products and services in development and production that include a significant increase in supply-chain security risk and mistargeting of tampered products and services.
- While there may be a framework for lawful interception on end-user devices, tampering, the example of targeted interception *(Page 9)* given in the background note does not include the condition of obtaining a warrant or similar permissive legal enabler, which might be interpreted as providing a carte blanche for states to carry out tampering without doing so within a legal framework. This norm should permit interception that is legal both in international and municipal law.
- In the second paragraph, the term "proper function" is not defined. "Proper function" of the internet might entail different objectives for the variety of state and non-state actors that have a crucial say, and should therefore be defined or clarified.
- This norm would not prohibit targeted state action that poses little risk to the overall stability of cyberspace; for example, the targeted interception and tampering of a limited number of end-user devices in order to facilitate military espionage or criminal investigations. It is unclear in the threshold what the threshold of 'little' or 'grave' risk is. This stems from the fact that the document fails to explain what it means by 'cyber stability' itself. The example of targeted interception given here does not include the condition of obtaining a warrant or similar permissive legal enabler, which might be interpreted as providing a carte blanche for states to carry out targeted surveillance without doing so within a legal framework. This norm should permit interception that is legal both in international and municipal law.
- Ideally, vulnerabilities should only be introduced or exploited post-production, and without the involvement of non-state actors. This also avoids the risk of including systemic modifications to technology which introduce deliberate weaknesses through software or hardware backdoors.
- The discussion on attacks taking place prior to a device reaching the market is repetitive. We would suggest this point be captured as "Such tampering can

take place at the design and manufacturing stage before it is released or during an update - with consequences for the public at large. The time between inserting a vulnerability, and activating the vulnerability for malicious use, can vary."

- "Non-state actors may in turn tamper with products and services as well, as their objectives may be aided by their ability to disrupt the stability of cyberspace." This is a vague statement and seems to treat non-state actors in one group. It is not clear that non-state actors are tampering with products and services because their objectives are aided by their ability to disrupt cyber space.
- The background attempts to give an example of a situation where the norm would not apply, pointing to interception and tampering to facilitate military espionage. *(Page 9)* It is important in such examples that the threshold of legality, necessity, and proportionality are brought in as there is a risk of legitimizing otherwise illegal actions or actions that are not inline with international human rights standards.
- "Therefore, those creating products and services must commit to a reasonable level of diligence in the designing, developing and delivering of products and services that prioritizes security and in turn reduces the likelihood, frequency, exploitability and severity of vulnerabilities." It would be useful for the norm to point to existing standards or norms that would meet a 'reasonable level of diligence" Due diligence-presently a state obligation in International Law is made up of two prongs-knowledge (including 'constructive knowledge) and capacity.

3. Implementation

- **Export Controls**

  The newest source of regulation in this space Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996)[8]. It was initially applicable to the conventional arms and dual-use weapons used for the production of weapons of mass destruction (WMD).[9] It was expanded in 1998 to include controls against strong encryption software and in 2013 evolved to also include surveillance and intelligence gathering software.by controlling the creation and use of hardware and software associated with intrusion software [10] Intrusion software was defined in the Wassenaar Arrangement as "software specially designed or modified to avoid detection by monitoring tools, or to defeat protective countermeasures" and the extracted data from a computer or network device modified "standard execution path" of a program to allow "the execution of externally provided instructions."[11]

[8] The Wassenaar Arrangement- On Export Controls for Conventional Arms and Dual-Use Goods and Technologies accessed November 18 2017, at <http://www.wassenaar.org/about-us/>

[9] *Ibid*

[10] "classes of hardware and software "specially designed or modified for the generation, operation or delivery of, or communication with 'intrusion software'",

[11] Garrett Hinck, Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research, *Lawfare,* January 5, 2018, accessed July 1, 2018, at

At the December 2017 meeting of the Wassenaar Arrangement,the United States successfully managed to negotiate exceptions based on research use to the existing export controls regime.[12] While these amendments act as a major boost for the cyber-security community, the definition of 'intrusion software' still remains relatively broad.[13]

The future of the Wassenaar Regime certainly depends on balancing the control of export of illegitimate cyber weapons with the incentivising of genuine security research. [14]This task is further complicated by weak enforcement mechanisms under the arrangement that vary considerably from one jurisdiction to another.[15] Despite that, both USA and Russia remain a part of this 41-nation-club which is a positive sign for the future of the regime. By enabling the amendments in December,2017, the regime has shown that it is flexible enough to balance the needs of the various nation states who are members of the Arrangement and through this flexibility, also keep the non-state lobbying groups such as the cyber-security community satisfied.[16]

The implementation of this norm certainly depends on effective co-operation with export control regimes such as the Wassenaar arrangement and the GCSC should conceptualize a framework for sustained co-operation with these mechanisms.

- **File integrity management and other accountability mechanisms**
  File and software integrity verification mechanisms can act as tools to record and trace if tampering of software and devices has taken place. It can act as a crucial accountability mechanism.

- **Trade agreements**

<https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research> [hereinafter Hinck]

[12] Shaun Waterman, The Wassenaar Arrangement's latest language is making security researchers very happy, *Cyberscoop,* December 20, 2017, accessed July 13, 2018, at <https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/> The list of amendments to the Wassenaar regime include#:

(a) With regard to the description of controlled software,replacement of the term 'specially designed' to operate or communicate with intrusion software with the term 'command and control' intrusion software
(b) The addition of an exception for software which creates updates authorized by the operator or owner of the computer system
(c)Addition of exemptions for controls that is involved in the development of intrusion software or in the development of software which operates, controls or delivers intrusion software
(d) An addition of a clarification note, which does not diminish the right of national authorities to ascertain the extent of compliance with the existing control regime.

[13] *Ibid*

[14] Fabian Bohnenberger, "The Proliferation of Cyber-surveillance technologies: Challenges and Prospects for Strengthened arms control" 3 *Strategic Trade Review* 4 (2017) 81-102

[15]Stewart Baker, Wassenaar, Cybersecurity, and Why European Officials Get Better Lunches than Americans, *Lawfare,* November 5, 2017, accessed January 4, 2018, at <https://lawfareblog.com/wassenaar-cybersecurity-and-why-european-officials-get-better-lunches-americans>

[16] See Basu A (2018) " The Potential for the Normative Regulation of Cyberspace:Implications for India"<https://cis-india.org/internet-governance/blog/the-potential-for-the-normative-regulation-of-cyberspace-implications-for-india>

Anti-tampering requirements can be placed while negotiating trade agreements similar to requirements against data localization. This could also be brought in within the WTO framework. As WTO has a clear enforcement mechanism, compliance by states is more likely.

- **Articulation of International standards that would meet define threshold such as that of 'reasonable levels of diligence'**
  International law has articulated a similar standard that has largely been universally recognised. The ILC Draft Articles on Liability for Transboundary Harm have laid down a due diligence obligation.[17] The Commentary articulates that a due diligence obligation requires reasonable efforts by a State to inform itself of factual and legal components that relate foreseeably to a contemplated procedure and to take appropriate measures in a timely fashion to address them."[18]

  The International Court of Justice has stated that due diligence is an obligation of conduct and not of result.[19] The due diligence standard should be evaluated on a two-pronged test - of knowledge and capacity.[20] The knowledge prong entails assessment of whether the state possessed the knowledge of a specific cyber attack or whether it ought to have known about the operation given the means at its disposal ('Constructive Knowledge')[21]. The capacity prong entails that the state make full use of its institutional, resource and territorial capacity to detect cyber threats and prosecute them, if need be. [22]

  The due diligence principle has also been flagged off by Tallinn Manual 2.0 *(Rule 7)* which "requires a state to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of and produce serious adverse consequences for other states."[23] The commentary does not lay down any guidelines on the duty of host states to prevent potential attacks, the duties of states through which the attack is routed and how the 'constructive knowledge' test applies to cyber operations.[24]At the same time, the Manual is clear that there is no duty to monitor cyber activities originating from their territory owing to surveillance concerns.[25] The lack of clear guidelines applying this obligation to cyberspace render it difficult for host states and the rest of the international

[17] Commentary to Draft Articles on Prevention of Transboundary Harm, at 71

[18] *Ibid*

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

[20] 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.

[21] Kimberley N. Trapp. "State Responsibility for International Terrorism. Problems and Prospects", 23(1) *European Journal of International Law* (2011), 67.

[22] Kimberley N. Trapp. "State Responsibility for International Terrorism. Problems and Prospects", 23(1) *European Journal of International Law* (2011), 67.

[23] Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare(Cambridge University Press ,2017)

[24] 1) Clearly defined cyber security policy and/or legislation, 2) Use of government funds to create nodal agencies responsible for cybersecurity, 3) Continuous communication if any hazardous cyber activities are detected, 4) Response to any requests for evidence by international bodies

[25] Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law, 112*(4)

community to determine whether due diligence obligations in cyberspace are being fulfilled.[26]

Going forward, the GCSC should engage and commission further research that looks at how these existing legal thresholds can be applied to cyberspace and how this might inform the implementation of these norms given the prevailing dynamics.

- **Regulation of spyware**
  There have been multiple instances of governments using spyware to target individual citizens or communities. For example, in 2016 and 2017 the use of such technologies by the Mexican government and the United Arab Emirates were uncovered.[27] Therefore, there is a need for governments to be increasingly vigilant of the sources of tools they purchase and in addition, ensure that they do not buy tools that might be used to conduct surveillance upon and unduly stifle dissent either in their own country or in other parts of the world.

- **Promotion of open technical standards and open source software**
  Open technical standards often form the backbone for the development of equipment and software that need to interoperate. Cryptographic communication protocols, for instance, can be designed in such a way as to detect non-compliance of participating middleboxes or endpoints.[28] There may be no way to achieve this level of security guarantee for all ICT infrastructure. In such cases, a lower (but still significant) level of trust in ICT can be gained when products are certified as being compliant with a specific open standard. Therefore, states can actionise the proposed norm by promoting the use and development of open technical standards, and encouraging buyers of equipment and users of ICT to consider whether a product is compliant with an open standard as a relevant factor for adoption.

  Similarly, open source software and hardware can increase trust in ICT since they open up the implementation details of the product to public scrutiny. States can encourage such software and hardware by incentivising contributions to them, or making policies that permit state departments to acquire only open source software and hardware for their own use.

  While these practices will not entirely eliminate detection of tampering with a particular piece of software or hardware, they can play a significant role in increasing general ICT security.

4. Supporting Documents

[26] Ibid

[27] https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

[28] *See, for instance*, E. Rescorla, et. al. (August 2018), “RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3”, Internet Engineering Task Force, <https://tools.ietf.org/html/rfc8446>

- Australia's Assistance and Access Bill 2018 enables Australian investigators to tamper with products and services for the purpose of accessing encrypted communications.[29] This is an example of concerning practice where legislation is legitimizing action that would run contrary to the norm. The Bill has been criticized for expanding the reach of government access and weakening security of communication systems.[30]
- Uchenna P. Daniel Ani, Hongmei (Mary) He & Ashutosh Tiwari (2017) Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, Journal of Cyber Security Technology, 1:1, 32-74

5. Examples

- The 2016 encryption debacle between Apple and the Federal Bureau of Investigations saw Apple being compelled by law enforcement authorities in the United States to write software which would systematically weaken or otherwise render useless the encryption of Apple iPhone devices. Apple did not comply with these requests. This is an example of an instance where deliberate weakening of security and cryptographic protocols would have had a clear impact on the integrity and security of Apple devices. A similar scenario - in the context of an encrypted text messaging app or email provider - would arguably have a direct impact on the stability of cyberspace.
- NSA was found to be implanting "beacons" into Cisco products.[31]

Norm Against Commandeering of ICT Devices into Botnets

"State and non-state actors should not commandeer others' ICT resources for use as botnets or for similar purposes."

1. Norm

The specificity in using "ICT resources for botnets" and the vagueness in "for similar purposes" in this norm could result in this norm being selectively too specific and too general for effective implementation. Further, The text is ambiguous in so far that it does not cover the use of self-owned ICT resources (i.e., resources which have been specifically commissioned and not "commandeered") for use as bots. We would suggest the

[29] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195

[30] https://cyberlaw.stanford.edu/files/publication/files/2018-10-11%20Pfefferkorn%20Comments%20to%20Joint%20Cmte%20on%20Asst%20%26%20Access%20Bill.pdf

[31] https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

following:

> **“State and non-state actors should not commandeer or commission ICT resources of civilians to facilitate or directly execute offensive cyber operations.”**

2. Background Notes

- The background covers botnets, use of malicious software, and the commandeering of ICT resources of civilians to facilitate or directly execute offensive cyber operations. As suggested in the text of this norm we would recommend harmonizing the scope of the background to ‘commandeer ICT resources of civilians to facilitate or directly execute offensive cyber operations.
- A significant amount of the background focuses on the harm that can arise out of the commandeering of ICT resources. We would recommend this be condensed into the following bullet points: 1. Online and offline safety issues 2. Negative impact on confidentiality, availability, and integrity of third party devices and its owner/operator including opening of further vulnerabilities and casting inappropriate liability on users.
- The example of instances potentially legitimate action needs to be qualified as cases of legal instances as there is the risk of legitimizing illegal actions. “The Commission recognizes that there are cases — for instance for law enforcement purposes — in which authorized state actors may find it necessary to install software agents on devices of a specifically targeted individual adversary, or a group of adversaries.” *(Page 10)* Reference to the need to justify the legality and legitimacy of these actions at every step is an imperative.

3. Implementation

- **Legislation and domestic policy measures**
  Many states are yet to develop domestic laws or updated cyber strategies that account for the changing dynamics of cyber security. Various states, particularly those states which are beginning to develop a workable digital economy, also do not have a cohesive cyber security ecosystem that enables co-operation between intelligence agencies, governmental nodal agencies responsible for protecting information infrastructure and other stakeholders in the cyber-security ecosystem such as the military. Therefore, the GCSC should work with state actors and legislators in countries across the globe to recommend legislation that allows for the development of this ecosystem.

- **Attribution processes and uniform evidentiary standards**
  One of the major challenges to the effective implementation of this norm and ensuring compliance with the standards it sets is the challenge of attribution in

cyberspace.[32] No technical routine can fully solve the problem of attribution in cyberspace.[33] However, without the possibility of credible attribution, it is unlikely that states and non-state actors will be sufficiently deterred to comply with the norm. Quality attribution depends not only on the effective use of skills and tools but also on a positive organisational culture, well run teams and cooperation across sectors, including among stakeholders that span multiple jurisdictions. This holistic approach to attribution can only be In this context, public communication regarding the attribution process become very important as it can foster public discourse on accountability standards and be a tool for cyber deterrence. [34]

- **Co-operative mechanisms and standards**
  States need to work together across jurisdictions to devise appropriate mechanisms through which they can respond in order to mitigate and, if necessary enact punitive measures against states or non-state actors that violate this norm. Relying on existing regional or economic coalitions, such as NATO, ASEAN or SAARC to develop these frameworks might be a potential starting point. These mechanisms could be used for dialogue, information-sharing and technical assistance-within the prevailing framework of International Law. Co-operation should be encouraged not only at the ministerial level but also between specific nodal authorities (such as Computer Emergency Response Teams-CERTs) that are responsible for the protection of information infrastructure across countries.

4. Supporting Documents

- UN ILC, 'Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities (with Commentaries)' (2006) GAOR 61st Session Supp 10, 106
- Davis, John S., Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern and Michael S. Chase. Stateless Attribution: Toward International Accountability in Cyberspace. Santa Monica, CA: RAND Corporation, (2017).
- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. May 11th 2017.

5. Examples

- A botnet christened Smominru has been using the WannaCry exploit—EternalBlue—to turn Windows servers into cryptocurrency miners. The

[32] See Basu A (2018) " The Potential for the Normative Regulation of Cyberspace:Implications for India"<https://cis-india.org/internet-governance/blog/the-potential-for-the-normative-regulation-of-cyberspace-implications-for-india> 25-33
[33] Thomas Rid & Ben Buchanan " Attributing Cyber Attacks," Journal of Strategic Studies, 38 (2015) 1-2, 4-37
[34] See Basu A (2018) " Lessons learned from US response to cyber attacks" The Hindu Business Line <https://www.thehindubusinessline.com/opinion/lessons-from-us-response-to-cyber-attacks-ep/article25372326.ece>

botnet has reportedly captured between $2.8-3.6 million worth of the Monero cryptocurrency.[35]

- In October 2016, Dyn was the target of a distributed denial of service attack from a botnet.[36] The 'Mirai' botnet was responsible for delivering a historic distributed denial of service attack by commandeering vulnerable Internet of Things ("IoT") devices.[37]

Norm for States to Create a Vulnerability Equities Process

"States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure."

1. Norm

- In addition to 'procedurally transparent frameworks" we suggest that substantive frameworks that facilitate transparency are also worked on and incorporated into the norm.
- It is unclear what the term 'flaws' refers to in the norm. The ambiguity in this term could act as casting a wider net for disclosure or could only add confusion in how to implement the norm.
- We would suggest using standardized language for information systems and technologies
- Instead of default presumption, we would suggest this be changed to a 'rebuttable presumption' as it requires an action based on an existing legal standard as opposed to a mindset.

We suggest the following text for the norm:

> **"States should create both procedural and substantively transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities they are aware of in information systems and technologies. The rebuttable presumption should be in favour of disclosure."**

2. Background Notes

[35] https://www.techrepublic.com/article/nasty-botnet-uses-wannacry-exploit-to-mine-cryptocurrency-from-your-servers/

[36] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[37] https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

While we feel that the rationale behind the proposed norm is adequate and comprehensive, the broad principles might not be sufficient to constitute guidance on what a robust Vulnerability Equities Process policy would contain.

Since we recommend rewording this norm to include substantive transparency in the framework for states publicly disclosing vulnerabilities, the background notes should also highlight the importance of the same. Specifically, the background notes should contain the importance of timely disclosure of vulnerabilities, concretely maintain that no vulnerabilities should be kept confidential indefinitely, and specific decisions about withholding public disclosure of a vulnerability should be reviewed periodically.

3. Implementation

As indicated above, we feel that implementing this norm would require two aspects. The research-driven aspect of this would be to develop a model set of standards on a vulnerabilities equities process that balances the need for disclosure with the benefits of not doing so. Second, is directly working with various state agencies to take inputs and help them put in a Vulnerabilities Equities Process in place through legislation or policy prescriptions.

4. Supporting Documents

- The Centre for European Policy Studies' report on software vulnerability disclosures in Europe highlights several actionable guidelines for implementing a robust vulnerability disclosure framework, which have general applicability to all states. Some of their recommendations are that the disclosure process be codified in law to ensure compliance, all decisions to withhold disclosure of a vulnerability should be reviewed at a fixed period (six months), and relevant standards bodies be involved when a discovered vulnerability may have an impact on physical security (say the vulnerability affects transport services or medical devices).[38]
- The Belfer Center's report which focuses on states' role in a Vulnerability Equities Process covers similar ground as the background note provided with this norm, but goes on to add that the high-level criteria for deciding whether a vulnerability will be disclosed should also be public. It also contains some recommendations similar to ones put forth by the Centre for European Policy Studies, specifically that the process should be backed by executive order and that all decisions to withhold publication of information regarding a discovered vulnerability be subject to a periodic review.[39]

[38] Marietje Schaake, et. al (June 2018), "Software Vulnerability Disclosure in Europe: Technology,Policies and Legal Challenges", Centre for European Policy Studies, <https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf>

[39] Ari Schwartz, et. al (June 2016), "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process", Belfer Center for Science and International Affairs, <https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Disclosure%20Web-Final4.pdf>

- The White House published a Vulnerabilities Equities Policy for the United States Government.[40]
- The UK Government, in November 2018, released its Vulnerabilities Equities Process which is operated by the Government Communications Headquarters (GCHQ).[41]
- Ari Schwartz and Sven Herpig cover the general principles and workflows of Vulnerabilities Equities Processes.[42]

5. Examples

- The National Security Agency (NSA) of the US has been criticised for not making timely public disclosures of vulnerabilities they discovered.[43]

Norm to reduce and mitigate significant vulnerabilities

"Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity."

1. Norm

This norm appears to be packing a lot of content into one norm-thereby casting a spider's web of obligations without delineating each one clearly. Various terms in this norm are unclearly defined. This includes the appropriate threshold for 'reasonable steps' and 'significant vulnerabilities' or "services on which the stability of cyberspace depends," which requires more elaboration, as it appears to be too broad. We recommend simplifying this norm by using the framing used in the 2015 UN-GGE Report

[40] The White House (November 2017), "Vulnerabilities Equities Policy and Process for the United States Government", Belfer Center for Science and International Affairs, <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>

[41] Government Communications Headquarters (November 2018), "The Equities Process", Government Communications Headquarters, <https://www.gchq.gov.uk/features/equities-process>

[42] Sven Herpig and Ari Schwartz (January 2019), "The Future of Vulnerabilities Equities Processes Around the World", Lawfare, <https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world>

[43] Lily Hay Newman (November 2017), "Feds Explain Their Software Bug Stash—But Don't Erase Concerns", Wired Magazine, <https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/>; Tim Cushing (August 2016), "Did The NSA Continue To Stay Silent On Zero-Day Vulnerabilities Even After Discovering It Had Been Hacked?", Techdirt, <https://www.techdirt.com/articles/20160818/11593035275/did-nsa-continue-to-stay-silent-zero-day-vulnerabilities-even-after-discovering-it-had-been-hacked.shtml>; Ellen Nakashima and Andrea Peterson (August 2016), " NSA's use of software flaws to hack foreign targets posed risks to cybersecurity", <https://www.washingtonpost.com/world/national-security/nsas-use-of-software-flaws-to-hack-foreign-targets-posed-risks-to-cybersecurity/2016/08/17/657d837a-6487-11e6-96c0-37533479f3f5_story.html>

with some modifications that also indicates mechanisms for implementation. Therefore, we recommend that the norm be amended to the following:

> **“States and non-state actors should encourage responsible and timely reporting and mitigation of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure. They should also work towards setting up a transparent process for regular evaluation of the process implemented to detect and mitigate vulnerabilities.”**

2. Background notes

“ … that prioritizes security and in turn reduces the likelihood, frequency, exploitability and severity of vulnerabilities.” Merely casting an obligation of prioritizing security may not be a strong enough obligation. Stronger wording such as ‘ensuring’ would be more appropriate.

3. Implementation

- To ensure that states and non-state actors carry out due diligence that ensures the basic security of their information systems, states must adopt and promote frameworks that helps developers of such systems to implement security safeguards, minimize risk in their information management processes, and evaluate their systems for minimum standards of security. For guidance, states can look at, for instance, the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 family of standards which provide internationally agreed-upon practices for information security management systems.
- We recommend that states develop adequate breach notification and incident reporting frameworks, and promote such frameworks for non-state actors as well.

4. Supporting Documents

- ISO/IEC 27000 family of standards which provide internationally agreed-upon practices for information security management systems.
- ISO 29147 outlines an approach to accepting vulnerability reports, and coordinated vulnerability disclosure.

Norm on Basic Cyber Hygiene as Foundational Defense

“States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.”

1. Norm

The norm in its present form does not clarify whether these laws and regulations should apply extraterritorially. Without this clarification, the norm appears to be justifying the extra-territorial application of domestic legislation, thereby leading to the casting of obligations on states not through the consensus-driven framework in international law but through municipal law in a few states. Further the threshold of ‘basic cyber hygiene’ should be defined or clarified. Therefore, we recommend that the norm be reworded to:

> **“States should enact appropriate measures, including laws and regulations, to ensure cyber hygiene within their territory”**

2. Background

“Moreover, these standards represent best practice, highlight the importance of sensible, regular oversight...” The use of the word ‘sensible’ in this sentence should be replaced with something more precise-such as ‘appropriate’ or ‘adequate’.

3. Implementation

Our recommendation here would be again to prescribe research on model standards for the laws and regulations envisaged by the norm but also go forward and see how these standards differ for states with differing levels of economic and technical capacity. Going forward, the GCSC should also conceptualize ways in which this gap can be bridged-by states or private actors and conceptualizing the role that the GCSC can play in aiding states at the lower end of the socio-economic spectrum.

4. Supporting Documents

- Review of Cyber Hygiene Practices. December 2016. European Union Agency for Network and Information Security.
- The SDG’s and Cybersecurity. New America.
- IGF 2017 - Best Practice Forum on Cybersecurity.

Norm Against Offensive Cyber Operations by Non-State Actors

“Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur.”

1. Norm

The wording of the norm is appropriate and comprehensive.

2. Background notes

The background is well drafted. We have two further suggestions. *First***,** with regard to active defense by the private sector, as we have argued elsewhere, it may be useful to follow a model of co-optation where where private sector actors, security researchers and commercial cyber-security researchers and professionals work with law enforcement authorities, military, and other nodal agencies responsible for cyber security as part of a multi-stakeholder unit. Decisions are taken by the unit as a whole rather than individual actors. The United States Cyber Command is an example of this.[44] It is one of the ten unified commands that come under the aegis of the United States Department of Defense.[45] Israel’s cyber strategy also involves an ecosystem approach which includes both passive and active defense and offensive capabilities across military domains.[46] Singapore’s Cyber Security Agency, which was set up in 2015 under the Prime Minister’s Office (PMO) was set up to protect critical information infrastructure and “coordinate efforts across government, industry, academia, businesses and the people sector, as well as internationally.”[47]

Second, the obligation to prevent stems from the obligation to prevent transboundary harm, which has been recognised by the International Court of Justice and the International Law Commission in its Draft Articles on Liability. As iterated above, due diligence obligation requires reasonable efforts by a State to inform itself of factual and legal components that relate foreseeably to a contemplated procedure and to take appropriate measures in a timely fashion to address them."[48] The International Court of Justice has stated that due diligence is an obligation of conduct and not of result.[49]

3. Implementation

[44]"Achieve and Maintain Cyberspace Superiority." Cybercom.mil. April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Vision April 2018.pdf?ver=2018-06-14-152556-010.

[45] "Mission and Vision." U.S. Cyber Command. https://www.cybercom.mil/About/Mission-and-Vision/.

[46] Raska, Micheal. "Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy." S. Rajaratnam School of International Studies. January 2015. Accessed November 2, 2018. https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_-Israel_Evolving_Cyber_Strategy_WEB.pdf.

[47] "Singapore's Cybersecurity Strategy." Cyber Security Agency of Singapore. 2016. Accessed November 2, 2018. https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf.

[48] *Ibid*

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

As mentioned above, the development of a cohesive attribution framework that incorporates uniform evidentiary standards and co-operation among states, private sector actors and security researchers is a must for the implementation of this norm.

4. Supporting Documents

- Wyatt Hoffman & Ariel E. Levite, Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyberspace?, https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf.
- "Firewalls and Firefights." The Economist. August 10, 2013. Accessed November 02, 2018. https://www.economist.com/business/2013/08/10/firewalls-and-firefights.
- Active Defence Task Force, "Into the Gray Zone: The Private Sector and Active Defence Against Cyber Threats", Centre for Homeland Security, George Washington University, October 2016. https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.
- Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," Stanford Journal of International Law 50, no. 1 (Winter 2014): 2.
- Basu, Arindrajit and Hickok, Elonnai, Conceptualizing an International Framework for Active Private Cyber Defense (December 9, 2018). Available at SSRN: https://ssrn.com/abstract=3298356or http://dx.doi.org/10.2139/ssrn.3298356
- UN ILC, 'Draft Principles on the Allocation of Loss in the Case of Transboundary Harm Arising out of Hazardous Activities (with Commentaries)' (2006) GAOR 61st Session Supp 10, 106

5. Examples

- Loosely worded policy documents that encourage the private sector to engage in 'proactive' cyber-security measures without charting out guidelines detailing how these measures are to be implemented or the limits on their use could also be considered orchestration. For example, India's 2013 Cyber Security Policy states "To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices."
- Cyber security companies CrowdStrike[50], FireEye[51], Hexis[52] and MITRE[53] have attempted to develop the Active Cyber Defense (ACD) industry by developing a range of solutions and articulating justifications for its legalization.[54]

[50] "Cybersecurity Solutions." Cyber Security Solutions, Endpoint Security - CrowdStrike. Accessed November 02, 2018. https://www.crowdstrike.com/solutions/.

[51] "Cyber Security Experts & Solution Providers." FireEye. Accessed November 02, 2018. https://www.fireeye.com/.

[52] Hexis Cyber Solutions. Accessed November 02, 2018. https://www.immixgroup.com/hexis/.

[53] "Resiliency." The MITRE Corporation. January 27, 2014. Accessed November 02, 2018. https://www.mitre.org/capabilities/cybersecurity/resiliency.

[54] Amanda N. Craig, Scott J. Shackelford, and Janine S. Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis," American Business Law Journal 52, no. 4 (Winter 2015).

- A burgeoning industry of cybersecurity companies are providing honeypots and more aggressive ACD services.[55] These ACD services are part of a rapidly expanding cybersecurity industry that might reach 248.26 billion by 2023, in which ACD services occupy a fair share.[56] 36 per cent of respondents to a survey conducted at the Black Hat Security conference claimed to have indulged in active cyber defense.[57] Due to fears of prosecution, many companies outsource their ACD measures to companies at home or abroad.[58] Some cybersecurity companies also reportedly set up entire divisions abroad so that they can engage in ACD measures that are at present, illegal in the United States.[59]

Proposals for new norms

Norm against use of information from non-state actors for offensive cyber operations

"States should not employ the ICT resources of non-state actors or coerce non-state actors that have operations in other jurisdictions for facilitating offensive cyber operations or espionage or conducting mass surveillance of foreign or its own citizens."

Background

The growth of information and communication technology has been supported by non-state actors, mainly private companies, that produce and develop software and hardware products (such as operating systems, microchips, network switches, routers, and other networking equipment). As cyberspace becomes a venue for exacting commerce and communication, large amounts of information is available to these private companies that may be used for legitimate business purposes. This information is usually available to private companies as a result of their services and contracts with other parties, and can include users' personal information, private communication, communication metadata and other sensitive information.

While such non-state actors can operate across national borders by engaging in international trade, they are usually legally registered in a single jurisdiction. The state,

[55] Whatt Hoffman & Ariel E. Levite, Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyberspace?, https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf.
[56] "Cybersecurity Market worth $248.26 Billion by 2023." Market Research Firm. Accessed November 02, 2018. https://www.marketsandmarkets.com/PressReleases/cyber-security.asp.
[57] "Firewalls and Firefights." The Economist. August 10, 2013. Accessed November 02, 2018. https://www.economist.com/business/2013/08/10/firewalls-and-firefights.
[58] Whatt Hoffman & Ariel E. Levite, Private Sector Cyber Defence: Can Active Measures Help Stabilise Cyberspace?, https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf.
[59] Michael Riley and Jordan Robertson "FBI Probes if Banks Hacked Back as Firms Mull Offensives," Bloomberg, December 30, 2014, http://www.bloomberg.com/news/articles/2014-12-30/fbiprobes-if-banks-hacked-back-as-firms-mull-offensives.

where such private companies are registered, can influence the operations of these private companies through domestic legislation. For instance, states can coerce private companies to share the information they have collected over the course of their business with state agencies as this information that may be considered valuable for espionage and offensive cyber operations.

While states may have an obligation to access and use such information for national security purposes or to comply with mutual legal assistance treaties, the collection of such information from private companies *en masse* can be severely detrimental to the stability of cyberspace. *First*, such operations erode public trust in the security of ICT. *Second*, they result in an inherently inequitable scenario whereby states which are host to a variety of private companies operating in foreign jurisdictions retain an entrenched advantage against states which do not. *Third*, knowledge of such operations or uncertainty around the existence of such operations can sour international relations and trade. *Fourth*, the means to establish such mass collection of information can often take the form of an architecture connected directly to the infrastructure of private companies; this opens up the possibility of malicious actors gaining access to the intercepted information.[60]

Relation to existing norms

The norm to avoid tampering relates to IT products and services in development and production, and the norm against commandeering of others ICT resources relates to the use deployed products for offensive cyber operations. As such, they only cover threats to the stability of cyberspace that arise from inserting or exploiting vulnerabilities in IT products and services. Thus, they are they are insufficient to cover threats arising from state intervention in the operations of non-state actors while the products and services function as expected.

Examples (and why norm is needed)

While the National Security Agency (NSA) in the USA is a public authority, it has multiple partnerships with private sector corporations including Microsoft, Intel, Verizon, Quest and AT&T.[61] The NSA intercepts data communication from these platforms and redirects the data to their data repositories.[62] One such repository is located in Utah and is recognised through its code name “Mainway” which has been acting as an amassment of two billion ’record events’ a day since 2010.[63]

[60] See, for instance, Tom Cross, *Exploiting Lawful Intercept to Wiretap the Internet*, Blackhat DC (2010), <https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-Lawfull-Intercept-slides.pdf>

[61] Slide displayed in Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*(Hamish Hamilton 2014) for a detailed explanation of the operational procedures

[62] *Ibid*, at pp.103.

[63] George Lucas, *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare* (Oxford University Press, 2014) ,pp.144

In conjunction with their private partners, the NSA is able to gain access to data generated in foreign territories through various programs.[64] BLARNEY is one such program which relied on the NSA's relationship with AT&T to gain access to "high capacity international fiber optic cables, switches and/or routers throughout the world."[65] The countries targeted by this program include Brazil, France, Germany, Greece, Italy, Japan, Mexico, South Korea and Venezuela .[66] A similar program by the name of FAIRVIEW engaged in similar practices with the aid of a 'corporate partner'. Its operation is made blatantly clear through a leaked slide which highlighted its unique aspects as "Access to massive amounts of data; Controlled by variety of legal authorities and Most accesses are controlled by partner." [67]

The NSA's surveillance endeavours also target data containing the content of communications gained directly from nine biggest internet companies.[68] Unlike other programs that used 'upstream' collection using fiber optic cables and other infrastructure, the PRISM programme enabled the NSA to directly obtain content from the servers of U.S. private Internet Service Providers.[69] The slide revealed by the Snowden leaks encourages the NSA operators to use both 'upstream' surveillance and the content garnered through the PRISM programme.[70]

The Snowden revelations also revealed enthusiasm among personnel at the GCHQ working on these programs, although the information available is not as detailed.[71] They operate the Tempora program which intercepts data on fibre-optic cables transmitting data between US and Europe.[72] This is important as the majority or fibre-optic cables carrying transatlantic data land in the UK.[73]

Even when such links between state security agencies and private companies are not established, even mere suspicion of *en masse* information transfer from private companies to state agencies can be detrimental to international relations and trade. In 2017, the US restricted its agencies from using Kaspersky over fears of surveillance from Russian intelligence agencies.[74] More recently, several countries have either already placed restrictions on the use of Huawei/ZTE equipment in their jurisdiction or are considering placing such restrictions, because of the companies' alleged links to Chinese

[64] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*(Hamish Hamilton 2014) for a detailed explanation of the operational procedures, pp. 102

[65] Ibid , at pp.103

[66] *Ibid, at pp.103*

[67] Slide *available at* Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*(Hamish Hamilton 2014), pp. 103

[68] Ibid, at pp.108

[69] Glenn Greenwald and Ewen McAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' *The Guardian* (7 June 2013) <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link> accessed 5th April 2018

[70] Slide available on Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton 2014)

[71] Ewen McAskill and others, 'GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications' *The Guardian* (21 June 2013) <www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 5th April 2018

[72] *Ibid*

[73] *Ibid*

[74]https://www.theguardian.com/technology/2017/sep/13/us-government-bans-kaspersky-lab-russian-spying

state agencies and consequent fear of espionage: the list includes New Zealand[75], Germany[76], the UK[77], Australia[78], and the US[79].

In light of these events, it is imperative that a norm adequately address threats to cyber stability that arise from states accessing information collected by private companies in the course of their business.

Norm for providing technical assistance

"In conjunction with non-state actors, states should engage in capacity-building measures with and provide technical assistance to states with lower economic and technical capacity in order to enable them to comply with the other norms."

Background

Cyberspace is an entangled phenomenon-that impacts and is impacted by a variety of stakeholders-individuals, corporations and states at various stages of development. As noted above, any vulnerability might be commandeered by malicious actors to damage information infrastructure and in certain cases have adverse impacts on a country's economic and social stability. It is therefore imperative that all states be equipped with the capability and know-how to ensure that there is cyber hygiene-both by conceptualizing and implementing an adequate framework and having the technical capability to implement it.As cogently argued by Broitman, Fidler and Morgus in the Briefings to the GCSC,the gap in capacity among states is particularly wide in the field of cutting edge technologies, which makes the lack of capacity a further obstacle in building norms that are enforceable and implementable by all.[80] Tikk and Kerttunen have suggested a " Cyber Marshall Plan, building robust national capacities and unprecedented transfers of ICTs...{to create} a climate of wealth, health and security."[81] In an analogous scenario in the case of climate change, normative convergence was possible only after the UN and other centralized coalitions worked towards enabling capacity-building across emerging economies. Broitman et al have also referred to cybercrime capacity building done in El Salvador by the United Nations Office on Drugs and Crime (UNODC), which " not only has the benefit of raising local capacity for implementing cyber commitments, but

[75] https://www.theguardian.com/business/2018/nov/28/new-zealand-blocks-huawei-5g-equipment-on-security-concerns
[76] https://www.wsj.com/articles/germany-explores-ways-to-exclude-huawei-from-5g-mobile-infrastructure-1154772 2800
[77] https://www.ft.com/content/6719b6b2-f33d-11e8-9623-d7f9881e729f
[78] https://www.bbc.com/news/technology-45281495
[79] https://www.express.co.uk/news/world/1064368/donald-trump-usa-china-trade-war-Huawei-zte-ban
[80] Broitman,Fidler and Morgus (2018),"Promoting an international security architecture for cyberspace" (GCSC Issue Brief 2, Briefings from the Research and Advisory Group)
[81] Eneken Tikk and Mika Kerttunen, "Cyber Treaty is Coming," Publications, Cyber Policy Institute, accessed April 20, 2018, http://cpi.ee/wp-content/uploads/2018/02/Cyber-Treaty-is-Coming-Tikk-Kerttunen.pdf.

also develops local institutional ability to collaborate across borders, and an appreciation of, and thus demand for cyber norms."[82]

The implementation of this norm can be through:

1. **Financial assistance** aimed at enabling states to hire experts, train individuals and purchase necessary defensive cyber technology,
2. **Capacity-Building:** Conducting workshops, skilling professionals-including IT staff, law enforcement officials, vendors and establishing a mechanism for information exchange facilitated by central co-ordination mechanisms set up by the UN or multi-stakeholder bodies like the GCSC. This would also include setting up forums that allow policy-makers to interact with their counterparts and technical experts from around the world to establish a framework for best practices. Further, the capacity-building measures should also focus on raising awareness among users-so that they might implement best practices at the end-user level,
3. **Co-operation and dialogue on developing national cyber security strategies, legal frameworks and policy ecosystems** that enable all states to optimize their prevailing capacity.

Relationship with other norms

While the norm has been identified in the background to some of the norms, we feel that the obligation to provide technical assistance should act as an independent norm of responsible behaviour. It is critical for the implementation of any norm or legislation that furthers cyber security. Without states in the more advanced stages of technical know-how and technical development aiding emerging economies, it will be very difficult to address the capability gap and implement or promote norms on cyber stability and cyber hygiene.

[82] Eneken Tikk and Mika Kerttunen, "Cyber Treaty is Coming," Publications, Cyber Policy Institute, accessed April 20, 2018, http://cpi.ee/wp-content/uploads/2018/02/Cyber-Treaty-is-Coming-Tikk-Kerttunen.pdf.