Signatories

Access Now
African Freedom of Expression Exchange (AFEX)
Association for Progressive Communications (APC)
Derechos Digitales
Enrico Calandro, Research ICT Africa
Forum of Incident Response and Security Teams (FIRST)
Fundación Karisma
Global Partners Digital (GPD)
Internet Society
Jokkolabs Banjul
Louise Marie Hurel, Igarapé Institute
Media Foundation for West Africa (MFWA)
R3D: Red en Defensa de los Derechos Digitales
Prof. em. Wolfgang Kleinwächter

Joint civil society feedback on the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security revised non-paper norms proposals

1. Introduction

Global cyber governance, including the protection of a secure and stable cyberspace cannot be limited to any one actor. Only collectively with non-state actors can traditional public actors, nation-states and multilateral forums address complex and transnational global cyber threats. Therefore, an inclusive approach to maintaining peace and stability in cyberspace is needed.

In order to support the implementation of the agreed UN GGE norms adopted in 2015,[1] we provide feedback below on the proposals which are part of the current Open-ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG").[2]

2. Overarching key messages

- The operationalisation, by which we mean the enforcement and implementation of existing norms, should be the focus of current efforts by both state and non-state actors.
- Implementation should take into account the impact on human rights, as humans are the ones impacted by cyberthreats, incidents and operations. This includes the differentiated impacts on people or groups in positions of marginalisation or vulnerability because of their sexual orientation or gender identity, ethnicity, race, and other social and cultural hierarchies. Therefore, states should encourage further analysis or promotion of the eleven voluntary norms of the 2015 GGE, including their gender dimensions.[3] To meaningfully interpret the 2015 norms in a gender-sensitive way, gender-sensitivity approaches should be included from the start and built into the beginning of future initiatives to operationalise the norms.
- The engagement of all relevant stakeholders including civil society, technical community and academia from a broad range of countries is essential because:
    - There is a range of challenges in implementing the agreed-upon norms, and civil society has an important role to play in overcoming them. To address these challenges effectively, civil society should play a role in:

---

[1] United Nations, General Assembly, UN Doc. A/70/174

[2] OEWG Revised non-paper (27 May 2020), https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf

[3] Allison Pytlak, Deborah Brown, "Why Gender Matters in International Cyber Security", Association of Progressive Communications and Reaching Critical Will, 2020, https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf

- Socialising the norms (the Global Commission on the Stability of Cyberspace provides one example as their report encompassed and reengaged with pre-existing norms);
- Supporting implementation of the norms through research and expert guidance informed by national contexts;
- Coordinating and convening other stakeholders—including the public sector—to increase their awareness and capacity for understanding the norms and complying with them;
- Providing a focus on human rights, human security, and the impact of norm compliance or norm transgressions on specific communities or people;
- Providing independent, fact-based, and credible oversight of norms implementation, such as the establishment of vulnerability disclosure processes (VDPs), or engaging in information sharing to build trust (which is currently lacking);
- Monitoring the implementation of norms, even if they are not binding, to provide accountability for norm transgression and thereby incentivising norm implementation;
- Accounting for local contexts; and
- Providing balanced, academic research into specific subject-areas.

- While states' engagement with industry actors is also important, civil society organisations, academia and technical communities can be particularly effective in filling the knowledge and skills gap, which may be lacking at the government level, to monitor the compliance of cyber norms.
- All stakeholders have a role to play in supporting states to implement the agreed-upon norms, which rely on trusted relationships, expertise, information sharing, and collaboration.

3. Our input

We have observed that there is support and interest in guidance on the agreed norms to help with their implementation. With this analysis in mind, we support the proposals which focus particularly on the implementation of norms, or which offer guidance on the implementation and observation of the existing GGE norms as the valid mechanisms to operationalise them.

Having analysed the proposals and identified synergies, we propose the following amendments in the revised non-paper,[4] based on Canada's proposal in the revised non-paper, which provides guidance on the implementation of each of the norms. Recommendations for integrating other proposals in the non-paper are also included where relevant. The first column of the table below includes the reference to the norm. The second column includes the guidance text provided by Canada in the revised non-paper. The third column provides suggested additions or changes to the norm (indicated in red), while the fourth column explains the rationale for the suggested changes. Finally, the fifth column refers to organisations and resources which, from the point of view of the contributors, support the implementation of an effective and/or human-centric approach to the operationalisation of the norm.

[4] OEWG Revised non-paper (27 May 2020), https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf

Norm	Original proposed guidance text	Suggested change/s	Rationale	Good practice
(a) *Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security; (2015 ¶13(a)).*	i. This norm is general in nature and does not require its own specific guidance. The implementation of the entire range of norms will contribute to implementing the objectives of this norm.	In interpreting this norm, states should recognise the importance of the interconnected nature of stability and security of ICTs and the enjoyment of human rights, and should take a collaborative approach to work with stakeholders. Therefore, in interpreting this norm, states should ensure that measures "to address security concerns on the Internet in accordance with their international human rights obligations to ensure the protection of all human rights online [...]".[5] States should comply with existing obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation. In doing so, they should incorporate perspectives from all relevant and affected stakeholders at the earliest stage of cyber security policy development to ensure a holistic consideration of the implications of cybersecurity measures (Czech Republic proposal).[6] In implementing this norm, states should recognise and consider the role of industry, academia and civil society when specifying and implementing the modalities of cooperation.[7]	Measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security have impacts on human rights and internet security. For example, measures that states take for monitoring and surveillance can weaken Internet security and violate rights to privacy, as well as data protection frameworks. Steps taken to increase stability and security should be outlined in cybersecurity strategies. This promotes transparency and supports the integration of stakeholders in their implementation.	

[5] Sheetal Kumar, Deborah Brown, Anriette Esterhuysen "Unpacking the GGE's framework on responsible state behaviour: Cyber norms"(2019): https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/

[6] OEWG Revised non-paper (27 May 2020), https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf

[7] "Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary", Civil Society and Disarmament: 2017, https://www.un.org/disarmament/publications/civilsociety/civil-society-and-disarmament-2017/

		States should encourage individual affected parties within a state to share with their direct counterparts in other states. Given the network governance approach that is the internet, cooperation should be encouraged at all levels. States should conduct a gender audit of national or regional cyber security policies to identify areas for improvement.[8] States should specifically acknowledge their obligations to uphold women's rights online, in the context of recognizing the applicability of international human rights law, because of the differential threats they experience due to cyber incidents.[9]		
(b) *In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences (2015 ¶13(b)).*	i. States could establish the national structures, policies, processes and coordination mechanisms necessary to facilitate careful consideration of serious ICT incidents and to determine appropriate responses. ii. Once those structures and processes are in place, States could develop ICT incident assessment or severity templates to evaluate and assess ICT	i. States could establish the national structures, policies, processes and coordination mechanisms necessary to facilitate careful consideration of serious ICT incidents and to determine appropriate responses in consultation with all other stakeholders in an open, inclusive and transparent process. ii. Once those structures and processes are in place, States could develop ICT incident assessment or severity templates to evaluate and assess ICT incidents.	The nature of cyberspace means that a wide range of stakeholders are relevant to evaluating and responding to ICT incidents, including, but not limited to, incident response teams and network operations. ICT incidents may also disproportionately affect vulnerable groups, and impact on human rights. Therefore,	Citizen Lab[10] ETH Zurich CSS[11] CiviCERT – The Computer Incident Response Center for Civil Society[12] FIRST[13]

[8] Allison Pytlak, Deborah Brown, "Why Gender Matters in International Cyber Security", Association of Progressive Communications and Reaching Critical Will, 2020, https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf

[9] Ibid

[10] https://citizenlab.ca/about/

[11] ETH Zurich CSS. Public Attribution of Cyber Incidents. Retrieved from: https://css.ethz.ch/en/services/digital-library/publications/publication.html/8bc88d23-b083-4d47-bb96-65565e8ad81f

[12] CiviCERT. CiviCERT Mission Statement. Retrieved from https://www.civicert.org/about/

[13] FIRST. FIRST Vision and Mission Statement. Retrieved from https://www.first.org/about/mission

	incidents. iii. Transparency about and harmonization of such templates by regional organizations could ensure commonality in how States consider ICT incidents and improve communication between States. Wherever possible, the templates should be in line with existing practices and avoid duplication. iv. When considering all relevant information in the case of an ICT incident, States should conduct research into possible gendered impacts, and work inclusively with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of women's rights.	States should avoid centralising the exchange of information regarding security incidents between government bodies only, and foster a culture of cooperation between security incident response teams embedded in all stakeholder groups. Incident response should promote the shortest path between those incident responders most able to stop negative impacts from the incident. iii. Transparency about and harmonization of such templates by regional organizations could ensure commonality in how States consider ICT incidents and improve communication between States and other actors. iv. When considering all relevant information in the case of an ICT incident, States should conduct research into possible gendered impacts, and work inclusively with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of the rights of women and people with diverse sexual orientations and gender identities and expressions. States should consider the impact of ICT incidents on the rights to freedom of expression, privacy and freedom of association and assembly, the rights of people with disabilities. All actors involved in cyber incident response (governmental, private sector, and civil society) should be equipped to recognize potential gendered impacts of an operation and respond appropriately, as well as conduct further research into those impacts to improve global understanding and knowledge;	we recommend there is recognition of this in the guidance.	

		Mechanisms and processes related to attribution should ensure respect for privacy, including by respecting data protection principles and frameworks. That includes ensuring that any access to information that might constitute protected information for the purpose of the fundamental right to privacy only takes place if it respects the international human rights standard of necessity and proportionality, including the specific standards and implementation guidance provided by the International Principles on the Application of Human Rights to Communications Surveillance. States must also act to ensure that they make their national strategies, policy documents, and other definitional instruments on ICT incident response and related issues publicly available for stakeholders to easily access and engage with. States should undertake to provide support to other states who may require further capacity building towards such efforts. States should also undertake to ensure that their national strategies, policies, and legal frameworks around ICT incident response and cybersecurity promote a vibrant culture of protecting independent security research. Specifically, States should help enable better collaboration with security researchers and other responsible information security actors, and not create legal uncertainty or fear of prosecution amongst them. States should avoid criminalization of cyber security expertise, including but not limited to research into security vulnerabilities, or exchange of information helpful to increase learning of security issues, or preventing their exploitation.		

(c) *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (2015 ¶13(c))*	i. With Respect To The Implementation of this norm: ● If a State identifies malicious cyber activity emanating from another State's territory or cyber infrastructure, a first step could be notifying that State. Computer Emergency Response Teams (CERTs) are crucial to being able to identify such activity. ● Given that ICT incidents can emanate from or involve third States, it is understood that notifying a State does not imply responsibility of that State for the incident. ● The notified State should acknowledge receipt of the request via the relevant national point of contact. ● When a State has knowledge that its territory or cyber infrastructure is being used for an internationally wrongful act that is likely to produce serious adverse consequences in another State, the former State should endeavor to take reasonable, available and	With Respect To The Implementation of this norm: ● If a State identifies malicious cyber activity emanating from another State's territory or cyber infrastructure, a first step could be notifying that State. Computer Emergency Response Teams (CERTs) are crucial to being able to identify such activity. ● Given that ICT incidents can emanate from or involve third States, it is understood that notifying a State does not imply responsibility of that State for the incident. ● The notified State should acknowledge receipt of the request via the relevant national point of contact. ● When a State has knowledge that its territory or cyber infrastructure is being used for an internationally wrongful act that is likely to produce serious adverse consequences in another State, the former State should endeavor to take reasonable, available and practicable measures within its territory and capabilities, consistent with its domestic and international law obligations, to cause the internationally wrongful act to cease, or to mitigate its consequences. ● This norm should not be interpreted as requiring a state to monitor proactively all	We recommend strengthening the reference to the measures that should be taken to mitigate the impact of malicious cyber activity, particularly as such activity is likely to result in data breaches and the infringement of the right to privacy. In addition, the norm should be interpreted to protect against abuses conducted by third parties, including business enterprises. This responds to the real, evidence-based threats which individuals face in cyberspace and which infringe on their rights.	EthicsfIRST[14] AfricaCERT[15] TF-CERT[16]

[14] Ethicsfirst. Ethicsfirst-About. Retrieved from http://www.ethicsfirst.org

[15] AfricaCERT. AfricaCERT Vision and Mission Statement. Retrieved from https://www.africacert.org/about-us/

[16] Geant. Community Taskforce – CSIRT. Retrieved from https://www.geant.org/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx

	practicable measures within its territory and capabilities, consistent with its domestic and international law obligations, to cause the internationally wrongful act to cease, or to mitigate its consequences. ● This norm should not be interpreted as requiring a state to monitor proactively all ICTs within its territory, or to take other preventative steps. ii. A State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond may choose to seek assistance from other States, including through standard assistance request templates. ● In such cases, assistance may be sought from other States, or from a private entity, in a manner consistent with national law	ICTs within its territory, or to take other preventative steps that contravene international human rights law, including the right to privacy. ii. A State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond may choose to seek assistance from other States, and cooperate with experienced international organisations, including through standard assistance request templates. ● In such cases, assistance may be sought from other States, or from a private entity, in a manner consistent with national law and international human rights law. Public-private-CSOs forms of collaboration, nationally and internationally, especially to take preventative actions; improve the capacity of incident response teams through a tailored approach to cyber capacity development; specialised training to build cyber capacity at all levels of States and across society: are all factors that can positively contribute to the implementation of this norm. This norm should also be interpreted to include that states must protect people against human rights abuses, including gender-based and other forms of violence, within their territory and/or jurisdiction by third parties, including business enterprises. For the prevention of internationally wrongful acts by third parties, states should develop and implement transparency measures to prevent abuses by private actors. States should hold private actors who enable or facilitate these acts to		

		account. States should take measures to protect human rights as part of their due diligence obligations. States should recognize that response to security incidents requires involvement from various stakeholders, not just national CERT/CSIRTs, and improve collaboration through training and capacity building with all stakeholder groups. States should encourage digital security training and other capacity building and assistance by stakeholders, including civil society, aimed at preventing security incidents, particularly to vulnerable communities and other users at risk. Retrospective reports of security incidents should be developed, shared and distributed while taking into account human rights and privacy, to improve global resilience against future security incidents.		
(d) *States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect. (2015 ¶13(d))*	i. In implementing this norm, States should: • Consider, as appropriate, supporting the work of the UN Commission on Crime Prevention and Criminal Justice, including the open-ended intergovernmental Expert Group, and its ongoing efforts to study, in a comprehensive manner, the problem of cybercrime. • Support the efforts of the	In implementing this norm, States should: • Consider, as appropriate, supporting the work of the UN Commission on Crime Prevention and Criminal Justice, including the open-ended intergovernmental Expert Group, and its ongoing efforts to study, in a comprehensive manner, the problem of cybercrime. • Support the efforts of the United Nations Office on Drugs and Crime to continue to provide, upon request and based on national needs, technical assistance and		

	United Nations Office on Drugs and Crime to continue to provide, upon request and based on national needs, technical assistance and sustainable capacity-building to Member States to deal with cybercrime, through the Global Programme on Cybercrime and, inter alia, its regional offices, in relation to the prevention, detection, investigation and prosecution of cybercrime in all its forms, recognizing that cooperation with Member States, relevant international and regional organizations, the private sector, civil society and other relevant stakeholders can facilitate this activity. • Consider taking new measures, such as adopting national legislation to combat cybercrime, in a manner that is consistent with States' human rights obligations and that ensures judicial guarantees.	sustainable capacity-building to Member States to deal with cybercrime, through the Global Programme on Cybercrime and, inter alia, its regional offices, in relation to the prevention, detection, investigation and prosecution of cybercrime in all its forms, recognizing that cooperation with Member States, relevant international and regional organizations, the private sector, civil society and other relevant stakeholders can facilitate this activity. Support should be provided towards the UNODC further investing resources on the use and improvement of Mutual Legal Assistance Treaty (MLAT) processes to help in combating cybercrime while protecting human rights. Additionally, colloboration should be encouraged between the UNODC and the UN Counter Terrorism Enforcement Directorate on knowledge sharing and harmonisation on international colloboration on combating cybercrime and other misuse of ICT in manners that respect human rights obligations. • Implement existing measures in a manner that is consistent with human rights obligations and consider taking new measures, such as adopting national legislation to combat cybercrime, in a manner that is consistent with States' human rights obligations and that ensures judicial guarantees and which ensures the safety of persons involved in legitimate security research activities. States should refrain from using cybercrime laws or other criminal laws to illegitimately restrict online expression, association and assembly. In implementing this norm, states must engage		

		meaningfully with multiple stakeholders, including civil society, academia and technical community,		
(e) *States, in ensuring the secure use of ICTs, should respect Human RightsCouncil resolutions A/HRC/RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age), to guarantee full respect for human rights, including the right to freedom of expression. (2015 ¶13(e))*	i. States should: ● Comply with their human rights obligations when designing and putting into place cyber security related initiatives or structures	i. States should: ● Comply with their international human rights obligations when designing and putting into place cyber security related initiatives or structures, employing a human centric approach, which includes respecting the conditions of necessity and proportionality. States should refrain from implementing initiatives, policy or legislation that would result in restrictions of human rights. Restrictions could only be permitted if the State can demonstrate the necessity and proportionality of such restrictions. States should refrain from employing unlawful or arbitrary surveillance techniques, including forms of hacking and malware, noting that concerns about public security may only justify the gathering and protection of certain sensitive information after they demonstrate the necessity and proportionality of such measures. States should ensure full compliance with their obligations under international human rights law in their collection of this sensitive information. Civil society is a key actor in promoting compliance with the human rights commitments. Hence, States should engage civil society at the earliest stage of implementation.	The integration of relevant Czech Republic proposals here would strengthen the guidance of this norm. In addition, greater specificity as to the types of measures which states employ and which undermine their ability to comply are now listed. The engagement of civil society, a key stakeholder in supporting state compliance with human rights obligations, is emphasised.	With regards to this norm, the resolutions referred to provide guidance on actions which states should take in order to comply with the resolutions. These include the adoption of comprehensive human rights legislation (or the existence of provisions in a constitution) which enable individuals to challenge acts which violate their human rights and obtain remedies. With regards to privacy and data protection, should adopt comprehensive legal frameworks in line with international best practice including Council of Europe's Convention No. 108 and the OECD Privacy Guidelines.

		States should comply with existing obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation (Czech Republic proposal) [17] States should prevent and mitigate discrimination risks in the design, development and, application of machine learning technologies and that ensure that effective remedies are in place before deployment and throughout the lifecycle of these systems States should incorporate perspectives from all relevant and affected stakeholders at the earliest stage of cyber security policy development to ensuring a holistic consideration of the implications of cybersecurity measures for human rights (Czech Republic proposal) [18] In order to comply with this norm, states could adopt national internet-related public policies that have the objective of universal access and enjoyment of human rights at their core (HRC Res. 26/13) and take steps to identify and bridge any digital divides that exist in the state (HRC 32/13). This includes adopting measures, including legislative measures, to ensure that persons with disabilities are able to access information and communications technology and systems on an equal basis with others (HRC 32/13) and promote digital literacy among		

[17] OEWG Revised non-paper (27 May 2020), https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf
[18] Ibid

		its population (HRC 26/13). The state should also prohibit measures which intentionally prevent or disrupt access to or dissemination of information online or publicly commit not to take such measures (HRC 32/13). It should also adopt a comprehensive legislative framework on surveillance and other investigatory powers, consistent with international standards and best practice, and which include independent oversight, grievance mechanisms and access to remedy (UNGA 68/167). States should adopt a comprehensive legislative framework on data protection with international standards and best practice and which include independent oversight, grievance mechanisms and access to remedy (UNGA 68/167).		
(f) *A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public (2015 ¶13(f)).*	i. States should: • Consider the potentially harmful effects of their ICT activities on the general functionality of global ICT systems and the essential services that rely on them.	State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the Internet, and therefore the stability of cyberspace (Netherlands proposal, modified)[19] State and non-state actors must not pursue, support or allow cyberoperations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites (Netherlands proposal)[20] States should consider medical services and medical facilities to be critical	The reference to "general functionality" and "essential services" should be further explained in order to support implementation.	

[19] Ibid
[20] Ibid

		infrastructure for the purposes of norms (Australia, Czech Republic, Estonia, Japan, Kazakhstan and United States of America proposal)[21] States should not conduct or knowingly support cyber activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm" (Czech Republic proposal)[22]		
(g) *States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions (2015 ¶13(g)).*	i. In order to contribute to a global culture of cybersecurity, States should consider, as appropriate, sharing information on best practices for protecting critical infrastructures, including all elements identified in this resolution and on: ● Baseline security requirements; ● Incident notification procedures; ● Incident handling tools and methodologies; ● Emergency resilience; and ● Lessons learned from previous incidents. ii. Capacity-building and other measures to build a global culture of cybersecurity should be developed inclusively and seek to	i. In order to contribute to a global culture of cybersecurity, States should consider, as appropriate, sharing information on best practices for protecting critical infrastructures, including all elements identified in this resolution and on: ● Baseline security requirements; ● Incident notification procedures; ● Incident handling tools and methodologies; ● Emergency resilience; and ● Lessons learned from previous incidents. ii. Capacity-building and other measures to build a global culture of cybersecurity should be developed inclusively and seek to address the gender dimensions of cyber security. iii. Given the varied and distributed nature of critical infrastructure ownership, ● States should, as appropriate, and in consultation with the relevant stakeholders, promote minimum standards for the security	The inclusion of civilian infrastructures and infrastructures essential to elections, referenda or plebiscites is to emphasise the the human-centric and rights-based approach to the governance of critical infrastructures	Cyberpeace Institute Meridian process (on CIIP) [24]

[21] Ibid

[22] Ibid

[24] Meridian Process. Meridian-GFCE Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers (2016). Retrieved from https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

	address the gender dimensions of cyber security. iii. Given the varied and distributed nature of critical infrastructure ownership, ● States should, as appropriate, and in consultation with the relevant stakeholders, promote minimum standards for the security of critical infrastructures and promote cooperation with the private sector, academia and the technical community in critical infrastructure protection efforts. iv. States should, as appropriate, participate in voluntary risk assessment and business continuity (resilience, recovery and contingency) planning initiatives involving other stakeholders and aimed at enhancing the security and resilience of national and cross-border critical infrastructure against existing and emerging threats	of critical infrastructures and promote cooperation with the private sector, academia and the technical community in critical infrastructure protection efforts. iv. States should, as appropriate, participate in voluntary risk assessment and business continuity (resilience, recovery and contingency) planning initiatives involving other stakeholders and aimed at enhancing the security and resilience of national and cross-border critical infrastructure against existing and emerging threats v. State and non-state actors must not pursue, support or allow cyberoperations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites (Netherlands proposal) [23] vi. Efforts to protect critical information infrastructures should be undertaken with due regard for applicable national laws concerning privacy protection and other relevant legislation. vii. Critical infrastructure should be governed in a way that is inclusive and rights-respecting. viii. In addition to assets that are essential for the functioning of a society and economy, critical infrastructure protection should include “soft” civilian infrastructures which support, and sometimes replace, the delivery of essential services and products for civilians, for instance supply chains for food provision		

[23] Global Commission for the Stability of Cyberspace (GCSC). Norm 8. Norm Against Offensive Cyber Operations by Non-State Actors (2018). Retrieved from https://cyberstability.org/norms/

		during periods of crisis, medical aid and also the provision of education.		
(h) *States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty (2015 ¶13(h)).*	I. Implementing this norm involves consideration of appropriate requests for assistance and consideration of the nature of assistance that can be offered in a timely manner. States receiving an appropriate request for assistance following an ICT incident should consider: • Acknowledging receipt of the request via the relevant national point of contact; • Determining, in a timely fashion, whether it has the capacity and resources to provide the assistance requested and respond; • In its initial response, indicating the nature, scope and terms of the assistance that might be provided, including a timeframe for its delivery; and • In the event that assistance is agreed upon, promptly providing the arranged assistance. Ii. Implementation of this norm would be further enabled by the prior existence of national structures and mechanisms, including a national point of contact, templates for assistance requests and confirmation of the assistance to be provided, and	Implementing this norm involves consideration of appropriate requests for assistance and consideration of the nature of assistance that can be offered in a timely manner. States receiving an appropriate request for assistance following an ICT incident should consider: • Designating a national point of contact for these requests; • Acknowledging receipt of the request via the relevant national point of contact; • Determining, in a timely fashion, whether it has the capacity and resources to provide the assistance requested and respond; this includes identifying the expertise in the country from a range of stakeholders • In its initial response, indicating the nature, scope and terms of the assistance that might be provided, including a timeframe for its delivery; and • In the event that assistance is agreed upon, promptly providing the arranged assistance. Ii. Implementation of this norm would be further enabled by the prior existence of national structures and mechanisms, including a national point of contact, templates for assistance requests and confirmation of the assistance to be provided, and through targeted capacity-building and technical assistance. • States should make sure that all relevant stakeholders are involved in the assessment of the request - this includes, but is not restricted to CERTs and National Cybersecurity Centres. This	This norm requires the effective collaboration of a range of stakeholders in order to implement. The additional text reflects this need, includes reference to CERTs and National Cybersecurity Centres, and provides further detail with regards to the processes and guidance that should be adopted in order to ensure ICT incidents are responded to in a timely and effective manner which respects human rights.	

	through targeted capacity-building and technical assistance. Bilateral and multilateral cooperation initiatives, international and regional organizations and fora can play a role in facilitating their development.	would avoid latency in response and further strengthen effective evaluation of capacities at their disposal to assist. • States should consider including different stakeholder groups in the assessment of requests according to the nature of the identified threat. • Adequate national understanding of available expertise and resources can further contribute to all stages of implementation of norm h - development of request, forwarding of the request to another state, acknowledgement of request and response. • States should have clear guidelines for the elaboration of requests in order to ensure consolidation of cooperation and trust. These requests partly imply in the identification of a particular malicious activity and therefore could include - to a certain degree - the attribution of a particular "malicious ICT act" directed towards critical infrastructures. • Bilateral and multilateral cooperation initiatives, international and regional organizations and fora can play a role in facilitating their development, including through sharing best practices on response and requests frameworks/templates. This could contribute to a better understanding and developing a voluntary baseline for the interpretation of what would be considered an "appropriate" request for assistance. • Recognise how the norm is dependent on a certain level of capacities, and that in order to ensure that the norm contributes to peace and stability in cyberspace as		

		well as responsible state behaviour, there is a need to recognise and address the different levels of capacities in responding/requesting assistance. • Ensure that requests for assistance, including relevant processes and resources such as frameworks/templates respect human rights, including the right to privacy.		
(i) *States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions (2015 ¶13(i)).*	To implement this norm, States should: • Take steps, including through existing fora, to prevent the proliferation of malicious ICT tools and techniques. In doing so, States should encourage the legitimate activities of research communities, academia, industry, law enforcement, CERTs/ CSIRTs and other cyber protection agencies in ensuring the security of their ICT systems.	To implement this norm, States should:- • Take steps, including through existing fora, to prevent the proliferation of malicious ICT tools and techniques. In doing so, States should encourage the legitimate activities of research communities, academia, industry, law enforcement, CERTs/ CSIRTs and other cyber protection agencies in ensuring the security of their ICT systems. Ensuring the integrity of the supply chain requires that states refrain from mandating backdoor access to ICT products (hardware and software) and, crucially, in popular communication platforms. Additionally, this norm is about preventing the proliferation of malicious ICTs and techniques as they put people at risk. States should implement vulnerability equities processes that avoid stockpiling tools and techniques that could be used for offensive operations. Businesses have the responsibility to respect human rights and ensure that their products and services are not used to violate human rights. States should be willing to share information about human	The suggested changes provide additional specificity to the measures required to ensure the integrity of the supply chain. Considering that supply chains require the engagement of industry actors who develop and oversee supply chains, it also includes suggested measures and processes, including existing processes, for engaging industry actors.	

		rights abuses by private actors and should hold private actors who enable or facilitate these acts to account. Companies should conduct rigorous human rights impact assessments on their products and policies.[25] States should integrate measures to support the integrity and security of ICT products into National Action Plans on Business and Human Rights (NAPs) are an important tool for supporting integrity and security of ICT products.[26]		
(j) *States should encourage responsible reporting of ICT vulnerabilities and share information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure (2015 ¶13(j))*	i. To implement this norm, States should: • Establish national structures that enable a responsible reporting and handling of ICT vulnerabilities; • Encourage appropriate coordination mechanisms amongst public and private sector entities; ii. In addition, and to avoid misunderstandings or misinterpretations, including those	i. To implement this norm, States should: • Establish national structures that enable a responsible reporting and handling of ICT vulnerabilities; • Encourage appropriate coordination mechanisms amongst public and private sector entities; ii. In addition, and to avoid misunderstandings or misinterpretations, including those stemming from non-disclosure of information about potentially harmful ICT vulnerabilities, States are encouraged to share, as appropriate, to the widest possible extent, technical information on	Additional guidance has been provided to highlight good practice in terms of transparency, accountability and stakeholder engagement in developing and implementing effective vulnerability disclosure processes.	ISO/IEC 29147:2018 and ISO/IEC 30111:2013[28] ENISA's Good Practice Guide in Vulnerability Disclosure[29] EthicsfIRST[30] FIRST Multi-Party Coordination and Disclosure guidelines[31]

[25] Sheetal Kumar, Deborah Brown, Anriette Esterhuysen "Unpacking the GGE's framework on responsible state behaviour: Cyber norms"(2019): https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/

[26] Ibid

[28] Information technology – Security techniques – Vulnerability disclosure. ISO/IEC 29147 (2018). Retrieved from: https://www.iso.org/standard/72311.html

[29] Information technology – Security techniques – Vulnerability handling processes. ISO/IEC 30111 (2013). Retrieved from: https://www.iso.org/standard/53231.html

[30] Ethicsfirst. Ethicsfirst-About. Retrieved from http://www.ethicsfirst.org

[31] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/

	stemming from non-disclosure of information about potentially harmful ICT vulnerabilities, States are encouraged to share, as appropriate, to the widest possible extent, technical information on serious ICT incidents, by using existing CERT to CERT coordination mechanisms, as well as mechanisms put in place by regional organizations (such as networks of points of contact). States should ensure that such information is handled responsibly and in coordination with other stakeholders, as appropriate	serious ICT incidents, by using existing CERT to CERT coordination mechanisms, as well as mechanisms put in place by regional organizations (such as networks of points of contact). States should ensure that such information is handled responsibly and in coordination with other stakeholders, as appropriate. Member States should be urged to consider the exchange of information on ICTs related vulnerabilities and/or harmful hidden functions in ICT products and to notify users when significant vulnerabilities are identified (NAM proposal) [27] States should ensure that inclusive processes for responsible state disclosure exist, that they do not criminalise security researchers, and that they are in line with good practice. To implement this norm, States should establish coordinated vulnerability disclosure policies or strategies, as well as structures that enable for the reporting and coordination of cybersecurity incidents, data security violations and vulnerabilities. Coordinated Vulnerability Disclosure policies should be clear, publicly available, and widely disseminated and communicated so that all stakeholders are cognizant of them and can act accordingly. These policies should at least contain guarantees for the protection and confidentiality of the identity and information related to the security researchers; identification of secure and reliable channels for		

[27] OEWG Revised non-paper (27 May 2020), https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf

		reporting; the type of events to be reported and those not to for using unethical discovery methods (e.g., DDoS attacks, social engineering); the stages of the process and timelines. Bodies or structures responsible for receiving and coordinating the reports should be neutral third parties, independent from national security and defence entities. The establishment of independent bodies avoid conflict with the general interest of a secure ecosystem vis-à-vis the potential interest of conserving and exploiting vulnerabilities for national security or defence (e.g., intelligence agencies often have a reason to exploit vulnerabilities; this requires the establishment of safeguards such as setting up independent bodies, setting up, and/or involvement of CERTs, etc.). Reward programs can take different forms from monetary payments to simple social media recognition of the security researcher who discovered the vulnerability. In the world of security research, this is an important incentive for collaboration and can help counteract the black market of zero-day vulnerabilities. Vulnerability reward programs should be joined by the development of strong vulnerability remediation processes, so issues reported can be rapidly mitigated and addressed		
(k) *States should not conduct or*	N/A	States should ensure that all CERTs/first responders are aware of this norm, and support its implementation.	The guidance here refers to the importance of engaging relevant actors in the	EthicsfIRST[33]

[33] http://www.ethicsfirst.org

knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.		States should ensure that the work of CERTs/First responders/National Cybersecurity Centres does not negatively affect the exercise of the rights of freedom of expression or privacy, among others.[32] States should prioritize building public trust in their national CERT/CSIRT, by: ● ensuring their independence from intelligence and law enforcement functions, or other functions that conflict with their duty to mitigate incidents; ● operate with transparency and in line with expectations from their constituency; ● that they are free to engage with counterpart CERT/CSIRT in other states in their role to investigate and mitigate security incidents. All CERT/CSIRTs, whether they operate with national responsibility or not should 1) be able to operate with independence from intelligence and law enforcement functions; or other functions that conflict with their duty to mitigate incidents 2) operate with transparency and 3) free to engage with counterpart CERT/CSIRTs in other states in their role to investigate and mitigate security incidents.	supporting its implementation, including the factors that need to be considered in order for computer emergency response teams or cybersecurity incident response teams	

[32] Sheetal Kumar and Klée Aiken, "Unpacking the GGE's framework on responsible state behaviour: Capacity building "(2019): https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-capacity-building/