IGF 2021

Best Practice Forum Cybersecurity

on the use of norms to foster trust and security

Mapping and Analysis of International Cybersecurity Norms Agreements

BPF WORKSTREAM 1 DRAFT REPORT - REFERENCES DOCUMENT

NOVEMBER 2021

2021 BPF Cybersecurity Workstream 1 Reference Materials – Cybersecurity Agreements

Main Report at https://www.intgovforum.org/en/filedepot_download/235/19829

Contents

i. African Union Convention on Cyber Security and Personal Data Protection

Agreement Overview			
I. Name of Agreement	**African Union Convention on Cyber Security and Personal Data Protection**		
II. Date it was signed/launched	**June 2014**	**III. Link**	https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**55**
VI. Organization responsible for ongoing management of agreement (if any)	**African Union**		
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Preamble	*"Reaffirming the commitment of Member States to fundamental freedoms and human and peoples' rights contained in the declarations, conventions and other instruments adopted within the framework of the African Union and the United Nations;"*
	1.2 Personal data	Art.8	*"Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data."*

2. Information security and resilience measures	**2.1CIP**	Art. 25.4	*"Protection of critical infrastructure* *Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technology systems designed to function in these sectors as elements of critical information infrastructure and… measures to improve vigilance, security and management"*
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	Art. 27.2	*"Each State Party shall adopt such measures as it deems necessary in order to establish appropriate institutions to combat cyber-crime, ensure monitoring and a response to incidents and alerts, national and cross-border coordination of cyber security problems, as well as global cooperation."*
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	Art 26.1	*"As part of the promotion of the culture of cyber security, State Parties may adopt the following measures: establish a cyber-security plan for the systems run by their governments; elaborate and implement programmes and initiatives for sensitization on security for systems and network users; encourage the development of a cyber-security culture in enterprises; foster the involvement of the civil society; launch a comprehensive and detailed national sensitization programme for Internet users, small business, schools and children.*
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	Art 29.1	*"Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety*

			guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers."
4. Cooperation and assistance	**4.1 General cooperation**	Art. 28.4	*"Means of cooperation* *State Parties shall make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between stakeholders. These means may be international, intergovernmental or regional, or based on public private partnerships."*
	4.2 Law enforcement assistance	Art 28.2	*"State Parties that do not have agreements on mutual legal assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability…"*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	Art. 29	*"Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code, or similar computerized data allowing access to part or all of a computer system."*
	5.4 Non-state actors	Art. 29	*State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to:*

			a) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized privileges.”
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	Art. 29	*“Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code, or similar computerized data allowing access to part or all of a computer system.”*
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	N/A	

ii. APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice

Agreement Overview			
I. Name of Agreement	**APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice**		
II. Date it was signed/launched	**May 2011**	**III. Link**	**https://www.apec.org/Publications/2012/03/APEC-Guidelines-for-Creating-Voluntary-Cyber-Security-ISP-Codes-of-Practice**

IV. Stakeholder groups party to the agreement	**Government**	**V. Total Signatories/supporters**	**21**
VI. Organization responsible for ongoing management of agreement (if any)	**Cybersecurity Policy and Asia Pacific Section** **Department of Broadband, Communications and the Digital economy**		

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	P.10, Sec 2	*"...it should be noted that ISPs should be encouraged to consider regulations and legislation pertaining to privacy for each economy. These should be taken into account when collecting and distributing information from networks. "*
2. Information security and resilience measures	**2.1 CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	P.5, Sec 2.6	*Registered ISPs that achieve the requirements set out in the code may also display a Trustmark to indicate their compliance with the code of practice on their website and in emails to their customers. The Trustmark could provide an online link to information about the code of practice to further increase consumer awareness of the provisions of the code.*

	2.5 Computer emergency response	P.10 Sec 4.2	***4.2 Methods for contacting affected users*** *If a compromised connection is detected, ISPs are encouraged to further investigate to verify the accuracy of any information recorded. Once satisfied that an affected user has been correctly identified, ISPs should notify the user. ISPs may consider notifying users by contacting them individually, as part of a group or by blocking or limiting their online access.*
	2.6 Incident mitigation	P.11, Sec 4.3	*"Once a compromised connection is detected and the affected user(s) are notified, ISPs are encouraged to provide remedial assistance. There is a range of remedial tools and services ISPs may deploy to assist affected users including:* ● *clear instructions on how to repair compromised computers manually;* ● *directing affected users to an anti-virus and/or security software vendor website;* ● *providing software specifically developed to assist with repairing compromised computers, often referred to as 'first-aid kits'; and onsite support."* *ISPs may also choose to quarantine the affected user's connection by restricting Internet access through a walled garden. A walled garden limits an affected user's Internet access and online services to:* ● *prevent any infection spreading to other users; and* ● *direct the affected user to specific content which could assist in resolving the compromised connection. This may include links to anti-virus software vendors' websites, links to relevant material on the ISP's own website, or access to an instant messaging service with technical support staff. "*
		P.7, Sec 3.1	***3.1 Educating consumers***

	2.7 Cyber hygiene		*ISPs who have agreed to comply with a cyber security code should be encouraged to raise the cyber security awareness of their customers. ISPs are best placed to distribute this information as they have a direct relationship with their customers and are in regular contact through network updates and billing*
		P.12, Sec 4.4	*“Therefore, the education and training of customer support staff is an important issue for ISPs. Moreover, larger ISPs have experience and expertise on information security issues and should be encouraged to assist small and medium sized ISPs to build their cyber security capabilities. “*
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	P.8, Sec 1	*“When a compromised connection exists on an ISP’s network, it is of benefit to the ISP to provide assistance to affected users and therefore restore the integrity of its networks. For a cyber security code of practice to function efficiently, ISPs need to be sufficiently engaged in managing their networks, notifying affected users and assisting in their recovery.”*
4. Cooperation and assistance	**4.1 General cooperation**	P.14, Sec 5.4	*“Despite the highly competitive ISP environment that exists in most APEC economies, from a business perspective there is significant benefit to implementing ISP cyber security initiatives simultaneously across the sector. Therefore, the existence of a separate coordinating body is likely to be very useful in the effective implementation of a code.* *A coordinating body would be responsible for encouraging, initiating and managing industrywide collaboration on cyber security. While the coordinating body may be the same as the responsible agency, it would be advantageous to have a separate entity which may be filled* *by regulators, Ministries, industry bodies or an independent ombudsman. Having members from the broader telecommunications*

			sector would allow the coordinating body to serve as a valuable distribution point which may be used to deliver network information ensuring that the privacy of users is protected, and to provide updates on other cyber security strategies deployed overseas and new remedial services and tools for ISPs." *"This strategy strongly encourages close collaboration with the private sector and with other international organizations."*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	P3, Sec 2.2	*These stakeholder groups included ISPs, and peak industry groups, government agencies and ministries, and Computer Emergency Response Teams (CERTs). Developing and implementing a voluntary ISP code of practice will not succeed without the commitment of at least the major ISPs*

	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	N/A	

iii. Arab Convention on Combating Information Technology Offences

Agreement Overview			
I. Name of Agreement	Arab Convention on Combating Information Technology Offences		
II. Date it was signed/launched	2010	**III. Link**	https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf
IV. Stakeholder groups party to the agreement	Government	**V. Total Signatories/supporters**	22 Arab League states
VI. Organization responsible for ongoing management of agreement (if any)	League of Arab States General Secretariat		
Norms Analysis			
Category	**Norms elements**	**Paragraph/citation**	**Quote from Text**

1. Rights and freedoms	**1.1 Human Rights**	Preamble	*"Adhering to the relevant Arab and international treaties and charters on human rights, and guaranteeing, respecting and protecting them."*
	1.2 Personal data	Art. 14	*"Offence Against Privacy Offence against privacy by means of information technology."*
2. Information security and resilience measures	**2.1 CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	N/A	
	4.2 Law enforcement assistance	Art. 34: mutual assistance agreements outside of existing, direct agreement.	*"The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested."*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	

5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	Art. 15	*"Offences Related to Terrorism Committed by means of information technology 1- Dissemination and advocacy of the ideas and principles of terrorist groups."*
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	Art. 12: Prohibition of pornography online.	*"Offence of Pornography 1- The production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that constitutes outrage of modesty through information technology."*

iv. ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)

Agreement Overview

I. Name of Agreement	**ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)**		
II. Date it was signed/launched	**July 2012**	**III. Link**	https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**10**
VI. Organization responsible for ongoing management of agreement (if any)	**The ARF Unit will review its implementation progress annually and report to the Inter-sessional Meeting on Counter Terrorism and Transnational Crime and to the Inter-sessional Support Group on Confidence Building Measures and Preventive Diplomacy.**		
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	

3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Sec.2 (i)	*“The voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations related to security of and in the use of ICTs as well as the procedures for this sharing of information;”*
		Sec.2 (ii)	*“Discussion exercises involving cooperation among ARF participating countries, on how to prevent incidents related to security of and in the use of ICTs becoming regional security problems;”*
		Sec.2 (iii)	*“Conduct of surveys on lessons learnt in dealing with threats to the security of and in the use of ICTs and creation of ARF databases on potential threats and possible remedies, taking into account the work that is already done in the commercial computer security sector and in the CERT community in this regard;”*
		Sec.2 (iv)	*“Capacity building related to security of and in the use of ICTs and to combating criminal use of the internet;”*
		Sec.2 (v)	*“Promotion of and cooperation in research and analysis on issues relevant to security of and in the use of ICTs;”*
		Sec.2 (vi)	*“Discussion on rules, norms, and principles of responsible behaviour by ARF Participating Countries and the role of cultural diversity in the use of ICTs;”*
		Sec.2 (vii)	*“Raising awareness for non-technical personnel and policy makers on threats in the use of ICTs and methods for countering such threats;”*
		Sec.2 (ix)	*“Discussion on the terminology related to security of and in the use of ICTs to promote understanding of different national practices and usage;”*
		Sec.2 (x)	*“Consideration of establishment of senior policy Point of Contacts between ARF Participating Countries to facilitate real time*

			communication about events and incidents in relation to security of and in the use of ICTs of potential regional security significance; and"
		Sec.2 (xi)	*"Consideration of establishment of channels for online information sharing on threats in ICT space, global ICT incidents and sources of ICT attacks threatening critical infrastructure, and development of modalities for real time information sharing (leveraging activities conducted by CERT networks)."*
	4.2 Law enforcement assistance	Sec.2 (viii)	*"Measures to promote cooperation among ARF Participating Countries against criminal and terrorist use of ICTs including, inter alia, cooperation between law enforcement agencies and legal practitioners, possible joint task force between countries, crime prevention and information sharing on possible regional cooperation mechanism;"*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	

	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	N/A	

v. ASEAN-United States Leaders’ Statement on Cybersecurity Cooperation

Agreement Overview			
I. Name of Agreement	**ASEAN-United States Leaders’ Statement on Cybersecurity Cooperation**		
II. Date it was signed/launched	**November 2018**	**III. Link**	https://asean.org/wp-content/uploads/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**Member States of the Association of Southeast Asian Nations (ASEAN) and the United States of America**
VI. Organization responsible for ongoing management of agreement (if any)	**ASEAN**		

Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**

1. Rights and freedoms	**1.1 Human Rights**	Para 11	*"Reaffirm that, as stated in UNGA resolution 71/199, the same rights that people have offline must also be protected online;"*
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Para 1	*"Commit to broadening and deepening our cooperation to promote an open, interoperable, reliable and secure ICT environment that fosters efficiency, innovation, communication and economic prosperity;"*
		Para 2	*"Reaffirm United Nations General Assembly (UNGA) resolution 71/28 and its call for all States to be guided in their use of ICTs by the 2015 Report of the UNGGE, including its recommendations to enhance trust, confidence and cooperation, as well as to promote an open, secure, stable, accessible and peaceful ICT environment;"*

		Para 5	*"Commit to promote certain voluntary, non-binding norms of responsible State behaviour in cyber space in peacetime, taking reference from the voluntary norms recommended in the 2015 Report of the UNGGE;"*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	whereas clauses	*"Noting that no State should conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;"*
		Para 8	*"Encourage economic growth through policies that build trust and confidence in the digital economy, such as but not limited to frameworks that strengthen consumer protection, intellectual property rights and cybersecurity, and promote effective personal data protection across jurisdictions, as well as policies in areas such as education and technology competency;"*
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	

	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	**Confidence Building**	Para 4	*“Commit to increase efforts in implementing practical confidence-building measures to reduce the risk of misperception and escalation, including through the ARF ISM on ICTs Security;”*
	Capacity Building	Para 6	*“Pledge to expand cooperation on the strengthening of cybersecurity that includes promoting regional capacity building programmes such as the ASEAN Cyber Capacity*
	Internet Governance	Para 9	*Encourage support for the multi-stakeholder approach to Internet governance, which involves active participation by governments and relevant stakeholders from across industry, academic, civil society and other domains;”*
	Digital Divide	Para 10	*“Resolve to bridge the digital divide and ICT development gaps within ASEAN, including for Least Developed Countries (LDCs) through developing digital competencies, market- driven approaches and policy cooperation along with the relevant regulatory framework; and promote efficient investment in digital infrastructure to drive robust, inclusive economic growth and prosperity;”*

vi. Charlevoix Commitment on Defending Democracy from Foreign Threats

Agreement Overview			
I. Name of Agreement	**Charlevoix Commitment on Defending Democracy from Foreign Threats**		
II. Date it was signed/launched	**June 2018**	**III. Link**	000373846.pdf (mofa.go.jp)
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**7**
VI. Organization responsible for ongoing management of agreement (if any)	**G7**		

Norms Analysis			
Category	**Norms elements**	**Paragraph/citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Art. 4	*“Share lessons learned and best practices in collaboration with governments, civil society and the private sector that are developing related initiatives including those that promote free, independent and pluralistic media; fact-based information; and freedom of expression.”*
	1.2 Personal data	Art. 5	*“Engage directly with internet service providers and social media platforms regarding malicious misuse of information technology by foreign actors, with a particular focus on improving transparency regarding the use and seeking to prevent the illegal use of personal data and breaches of privacy.”*
	2.1 CIP	N/A	

2. Information security and resilience measures	**2.2 Essential services**	N/A	
	2.3 Electoral processes	Art. 1	*“Respond to foreign threats, both together and individually, in order to meet the challenges facing our democracies.”*
	2.4 Public trust	Art. 6	*“Support public learning and civic awareness aimed at promoting critical thinking skills and media literacy on intentionally misleading information, and improving online security and safety.”*
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Art. 2 Art. 3	*“Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state.”* *“Establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for coordinated response”*
	4.2 Law enforcement assistance	Art. 7	*“In accordance with applicable laws, ensure a high level of transparency around sources of funding for political parties and all types of political advertising, especially during election campaigns.”*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
	5.1 Developing and deploying cyber weapons	N/A	

5. Restraint on development and use of cyber capabilities	**5.2 Intellectual property**	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	Art. 5	*"Engage directly with internet service providers and social media platforms regarding malicious misuse of information technology by foreign actors, with a particular focus on improving transparency regarding the use and seeking to prevent the illegal use of personal data and breaches of privacy."*
Any other norms areas included?	**Democratic Values**	Preface, Para 2	*"Democracy and the rules-based international order are increasingly being challenged by authoritarianism and the defiance of international norms. In particular, foreign actors seek to undermine our democratic societies and institutions, our electoral processes, our sovereignty and our security."*

vii. Commonwealth Cyber Declaration

Agreement Overview	
I. Name of Agreement	**Commonwealth Cyber Declaration**

II. Date it was signed/launched	**2018**	**III. Link**	**https://thecommonwealth.org/commonwealth-cyber-declaration**
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**54**
VI. Organization responsible for ongoing management of agreement (if any)	**Commonwealth Secretariat**		

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	Preamble	*“Building on the principles expressed in the 2014 Commonwealth Cyber governance Model adopted by the Commonwealth ICT Ministers Forum and our shared commitment to Commonwealth values of human rights, tolerance, respect and understanding, freedom of expression, rule of law, good governance, sustainable development and gender equality;”*
	1.2 Personal data	Sec. 3	*“Highlight the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data.”*
2. Information security and resilience measures	**2.1 CIP**	Preamble	*“Recognising the threats to stability in cyberspace and integrity of the critical infrastructure and affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks;”*
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	

	2.4 Public trust	Sec. 3	*“Highlight the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data.”*
	2.5 Computer emergency response	Sec. 2	*“Highlight the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime.”*
	2.6 Incident mitigation	Sec. 2	*“Highlight the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime.”*
	2.7 Cyber hygiene	Sec. 4	*“Encourage investment in cybersecurity and cyber hygiene skills, and to develop skills in the workforce, particularly for women and girls, and public awareness to help the public adopt secure online behaviours and protect themselves from cybercrime.”*
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	Sec. 1	*“Commit to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures”*
4. Cooperation and assistance	**4.1 General cooperation**	Sec. 1	*“Commit to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures.”* *“Commit to the establishment of effective and proportionate domestic cybercrime and cybersecurity frameworks that take into account*

			principles in existing international instruments, acknowledging the evolving tactics of cybercriminals and the transnational nature of cybercrime. Commit to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime"
	4.2 Law enforcement assistance	Sec. 1	*"Highlight the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime."* *"Recognise the potential for sharing of information across the Commonwealth for improving cooperation between government, law enforcement and industry, with due regard for necessary and proportionate safeguards"* *"Commit to the establishment of effective and proportionate domestic cybercrime and cybersecurity frameworks that take into account principles in existing international instruments, acknowledging the evolving tactics of cybercriminals and the transnational nature of cybercrime. Commit to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime"*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	

	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	Sec. 2	*"Highlight the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime."*
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**		*"Commit to limit the circumstances in which communication networks may be intentionally disrupted, consistent with applicable international and domestic law.* *Underscoring our shared interest in protecting the security of our networks, security of data, the people that use them, and the services that run on them;"*
Any other norms areas included?	***Description:***	N/A	

viii. Contract for the Web

Agreement Overview

I. Name of Agreement	Contract for the Web		
II. Date it was signed/launched	November 2019	**III. Link**	https://contractfortheweb.org/
IV. Stakeholder groups party to the agreement	Multistakeholder	**V. Total Signatories/supporters**	See: https://contractfortheweb.org/
VI. Organization responsible for ongoing management of agreement (if any)	Web Foundation		

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	Principle 3	*“Respect and protect people’s fundamental online privacy and data rights So everyone can use the internet freely, safely, and without fear”*
	1.2 Personal data	Principle 5	*“Respect and protect people’s privacy, personal data, and other online data rights to build online trust”*
2. Information security and resilience measures	**2.1 CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	Principle 5	*“Respect and protect people’s privacy, personal data, and other online data rights to build online trust”*
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	

	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	N/A	
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	Principle 6	There is no direct reference to due diligence, but in reference to Principle 6 *([Companies will]: Develop technologies that support the best in humanity and challenge the worst)* there is reference to relevant text from the UN Guiding Principles on Business and Human Rights and Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	Principle 9	*"Fight for the Web So the Web remains open and a global public resource for people everywhere, now and in the future By being active citizens of the Web:* *a. Creating awareness amongst peers regarding threats to the open Web.* *b. Opposing the Web's weaponization by nation states or any other entity.* *c. Supporting organizations, processes and people who promote the open Web.* *d. Supporting startups and established companies that espouse the Web's future as a basic right and public good.* *e. Engaging political representatives and companies to ensure support and compliance with this Contract and support for the open Web."*

	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	Principle 1 Principle 2 Principle 4	*[Governments will] “Ensure everyone can connect to the internet So that anyone, no matter who they are or where they live, can participate actively online”* *“Keep all of the internet available, all of the time So that no one is denied their right to full internet access”* *“Make the internet affordable and accessible to everyone So that no one is excluded from using and shaping the Web”*
	5.9 Election infrastructure		N/A
	5.10 Harmful hidden functions		N/A
6. Technical/Operational	**6.1 Network Security Practices**		N/A
Any other norms areas included?	***Description:***		N/A

ix. Convention on International Information Security (Draft)

Agreement Overview

I. Name of Agreement	Convention on International Information Security		
II. Date it was signed/launched	September 2011	**III. Link**	https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666
IV. Stakeholder groups party to the agreement	Government	**V. Total Signatories/supporters**	None – draft only
VI. Organization responsible for ongoing management of agreement (if any)	Ministry of Foreign Affairs of the Russian Federation		
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Art. 5	*"17) each State Party guarantees freedom of speech and expression in its information space, as well as protection against illegal interference into the private lives of citizens;* *18) each State Party aims to maintain a balance between fundamental human rights and the effective counteraction of terrorist use of the information space;"*
		Preamble	*"keeping in mind the necessity of ensuring the appropriate balance between maintaining law and order and protecting fundamental human rights, as foreseen in the 1966 International Covenant on Civil and Political Rights, as well as other international human rights*

			agreements, which assert the right of each individual to freely hold his or her own ideas, and to freely express these ideas and opinions, including the freedom to seek, receive, and distribute any kind of information or idea, regardless of national borders”
	1.2 Personal data	Preamble	*“keeping in mind also the right to a private life and the protection of personal data,”*
2. Information security and resilience measures	**2.1 CIP**	Preamble	*“actively integrate a stable global culture of cybersecurity, as is noted in the 21 December 2009 resolution A/RES/64/211 of the General Assembly of the United Nations "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures"”*
	2.2 Essential services	N/A	
	2.3 Electoral processes	Art. 5/Main principles of Ensuring International Information Security	*“ observe the following principles: 1) the activities of each State Party in the information space must promote social and economic development and must be consistent with the goals of maintaining world peace and security, and conform to the universally recognized principles and norms of international law, including the principles of peaceful reconciliation of strife and conflict, of the non-use of force in international relations, of* ***non-interference into the internal affairs of other States****, and of respect for the sovereignty of States and the major human rights and freedoms;”*
	2.4 Public trust	Preamble	*“acknowledging that trust and security when using information and communication technologies is a fundamental basis of the information society”*
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	

3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Chapter 2/Avoid conflict	*“ cooperate to ensure international information security to maintain world peace and security and to contribute to global economic stability and progress, general welfare of the peoples of the world and discrimination-free international cooperation;”*
	4.2 Law enforcement assistance	Chapter 4/Main measures	*“7) take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to collect or record information by means of technology in its territory as well as to demand similar action from service providers carried out continuously and in cooperation with the law enforcement authorities of the States;”*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	Article 5/Main Principles	*“16) each State Party will, within the limits of its means, ensure that fundamental human rights and freedoms, and the rights and freedoms of citizens, and intellectual property laws, including patents, technologies, commercial secrets, brands, and copyrights, are adhered to in its information space;”*
	5.3 Non-proliferation	Chapter 2/Avoid conflict	*“ take action aimed at limiting the proliferation of "information weapons" and the technology for their creation.”*
	5.4 Non-state actors	Chapter 3/Article 8	*“The States Parties acknowledge the possibility of the information space being used for carrying out terrorist activities”*
	5.5 Botnets	N/A	

	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:*** *Avoiding military conflict in cyberspace.* *Validity of international and domestic law in information transfers.*	Chapter 2/Article 6 Article 4/Threats	*" the States Parties shall take steps to anticipate and expose potential conflicts in the information space and take joint action to avert them and resolve crises and disputes peacefully"* *" the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved;"*

x. Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document

Agreement Overview			
I. Name of Agreement	**Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document**		
II. Date it was signed/launched	**2015**	**III. Link**	https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**38**
VI. Organization responsible for ongoing	**Organization for Economic Cooperation and Development (OECD)**		

management of agreement (if any)			
		Norms Analysis	
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Sec. 1.3 (Pg. 9)	*All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.*
	1.2 Personal data	Sec. 1.3 (Pg. 9)	*"Digital security risk management should be implemented in a manner that is consistent with human rights and fundamental values recognised by democratic societies, including the freedom of expression, the free flow of information, the confidentiality of information and communication, the protection of privacy and personal data, openness and fair process."*
2. Information security and resilience measures	**2.1CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	Sec. 2.A (Pg. 11)	*"National strategies for the management of digital security risk should be consistent with the Principles and create the conditions for all stakeholders to manage digital security risk to economic and social activities and to foster trust and confidence in the digital environment."*
	2.5 Computer emergency response	Sec. 2.B.1 (Pg. 12)	*"Ensuring the establishment of one or more Computer Security Incident Response Team (CSIRT), also known as Computer Emergency Response Team (CERT), at national level and, where appropriate, encourage the emergence of public and private CSIRTs working collaboratively, including across borders."*

	2.6 Incident mitigation	Sec. 2.B.4 (Pg. 14)	*"Fostering co-ordination among stakeholders to improve identification and remediation of vulnerabilities and threats, as well as mitigation of digital security risk;"*
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	Sec. 2.B.3 (Pg. 14)	*"Encouraging the responsible discovery, reporting and/or correction of digital security vulnerabilities by all stakeholders;"*
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 7	*"Calls on governments and public and private organisations to work together to empower individuals and small and medium enterprises to collaboratively manage digital security risk;"*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	

	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	N/A	

xi. DNS Abuse Framework

Agreement Overview			
I. Name of Agreement	**DNS Abuse Framework**		
II. Date it was signed/launched	**October 2019**	**III. Link**	**https://dnsabuseframework.org**
IV. Stakeholder groups party to the agreement	**DNS Registries and registrars**	**V. Total Signatories/supporters**	**48**
VI. Organization responsible for ongoing management of agreement (if any)	**DNS Abuse Institute (PIR)**		

Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Pg. 3	*'Despite the fact that registrars and registries have only one blunt and disproportionate tool to address Website Content Abuse, we believe there are certain forms of Website Content Abuse that are so egregious that a registry or registrar should act when provided with specific and credible notice. Specifically, even without a court order,[9] we believe a registry or registrar should act to disrupt the following forms of*

			Website Content Abuse: (1) child sexual abuse materials ("CSAM"); (2) illegal distribution of opioids online; (3) human trafficking;10 and (4) specific and credible incitements to violence. Underlying these Website Content Abuses is the physical and often irreversible threat to human life. Additionally, each registrar and registry has its own acceptable use policies or terms of use that set forth provisions that may cover these and additional forms of Website Content Abuses.'
	1.2 Personal data		
2. Information security and resilience measures	**2.1 CIP**	Pg. 1	*'The Domain Name System (DNS) serves as a crucial but largely unheralded system underpinning the Internet's ability to connect its users and devices. The safe and secure operation of the DNS has provided a firm foundation for the growth of the Internet as a global public resource, but much like the Internet as a whole, it is not immune to abuse. For the good of the Internet and everything it enhances, the undersigned domain name registrars and registries aim to reinforce the safety and security of the DNS by highlighting shared practices toward disrupting abuse of the DNS (DNS Abuse).'*
	2.2 Essential services		
	2.3 Electoral processes		
	2.4 Public trust	Pg. 5	*'The authors of this document are committed to bettering the DNS by making it a more trusted space and encourage other registries and registrars and the community to join us in these efforts.'*
	2.5 Computer emergency response		
	2.6 Incident mitigation	Pg. 2	*'We believe registrars and registries must act upon these categories of DNS Abuse. gTLD registries and registrars are required by our agreements with ICANN to maintain abuse contacts (and preferably a webform) to receive abuse complaints and to promptly investigate allegations of DNS Abuse in good faith. In addition, each of the undersigned disrupts DNS Abuse when identified within our registrations and encourages others to do the same.'*
	2.7 Cyber hygiene		

3. Reliability of products	**3.1 Supply chain**		
	3.2 Reporting of vulnerabilities		
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 4	*'Registrars and registries should promptly investigate allegations of DNS Abuse and the Website Content Abuse that falls within this framework. This requires coordination and good faith cooperation between the registrar and registry to balance the potential harm from the remedy against the harm caused by the abuse. When a registry identifies abuse, it should always provide notice to the registrar, given the registrar's closer business or contractual relationship with the registrant.'*
	4.2 Law enforcement assistance		
	4.3 CIP assistance		
	4.4 Due diligence		
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**		
	5.2 Intellectual property		
	5.3 Non-proliferation		
	5.4 Non-state actors		
	5.5 Botnets	Pg. 2	Botnets is one of five broad categories of harmful activity that together compose the signatories definition of DNS Abuse, and upon which registries and registrars *must* act.
	5.6 CIP		
	5.7 CERTs/CSIRTs		
	5.8 Internet		The definition of DNS Abuse is part of the agreement: *'DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and*

			spam (when it serves as a delivery mechanism for the other forms of DNS Abuse).'
	5.9 Election infrastructure		
	5.10 Harmful hidden functions		See 5.8 above – definition of DNS Abuse.
6. Technical/Operational	**6.1 Network Security Practices**		
Any other norms areas included?	***Description:***		

xii. Draft EAC Legal Framework for Cyberlaws

<table>
<tr><th colspan="4">Agreement Overview</th></tr>
<tr><td><b>I. Name of Agreement</b></td><td colspan="3"><b>Draft Eac Legal Framework for Cyberlaws</b></td></tr>
<tr><td><b>II. Date it was signed/launched</b></td><td><b>November 2008</b></td><td><b>III. Link</b></td><td>http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq</td></tr>
<tr><td><b>IV. Stakeholder groups party to the agreement</b></td><td><b>Governments</b></td><td><b>V. Total Signatories/supporters</b></td><td><b>N/A</b></td></tr>
<tr><td><b>VI. Organization responsible for ongoing management of agreement (if any)</b></td><td colspan="3"><b>East African Community Task Force on Cyber Laws</b></td></tr>
</table>

Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**

1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	Pg. 18 (Sec 2.5)	*"The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area (R.19)."*
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	Pg. 16 (Sec 2.4)	*"The objective of consumer protection rules in a cyberspace environment should be to facilitate eCommerce, from a demand-side, by engendering trust among consumers and thereby encouraging them to enter into online transactions. However, the imposition of substantial additional obligations upon online vendors should avoid becoming a legal obstacle to the provision of transactional activities.* *The following measures have been widely adopted internationally to provide a clear level of protection for consumers in a cyberspace environment:* *Information requirements – Vendors should be obliged to make readily available to consumers a range of information concerning the identity of the vendor, the nature of the transactions, the process by which the transaction is entered into and all the associated costs to be paid by the consumers, including applicable taxes and delivery costs. 6 See Annex II. 7 See Article 37, 'Accession to the Convention'.* • *Cancellation right – A consumer should be granted the right to cancel a contract for certain*

			types of goods and services, without reason and within a specified time period. - *Payment fraud – A consumer should be granted certain protections from liability for fraudulent payments made in the consumer's name, unless the vendor or payment service provider can prove that the consumer has been grossly negligent in the operation of the payment mechanism.* *Performance obligations – The vendor should be obliged to perform the contract within a minimum specified period of time or be liable to fully refund the consumer."*
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	N/A	
	4.2 Law enforcement assistance	Pg. 16 (Sec 2.3.2)	*"The Task Force recommends the following:* *That the EAC Secretariat considers the possible role of the Court of Justice in addressing the multi-jurisdictional nature of computer crime and the adoption of common criminal procedures within the EAC"*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
	5.1 Developing and deploying cyber weapons	N/A	

5. Restraint on development and use of cyber capabilities	**5.2 Intellectual property**	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	Pg. 14 (Sec 2.3.1)	*"In terms of offences targeting the confidentiality, integrity and availability of computer or information systems and the data they process, there is broad consensus around the types of conduct that should be criminalised:* • *Unauthorised access to the system* • *Unauthorised interference or modification of the system or the data processed on the system* • *Unauthorised interception of communications between or within systems;* • *Misuse of devices, including the supply or possession of tools such as password cracking or virus writing software.* *Measures designed to tackle cyber-terrorist or cyber-warfare conduct are based around the motivation of the offender rather than his conduct, which will generally fall within one of the four categories above"*
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	

Any other norms areas included?	***Description:***	N/A	

xiii. Ethics for Incident Response and Security Teams (EthicsfIRST)

Agreement Overview			
I. Name of Agreement	**Ethics for Incident Response and Security Teams (EthicsfIRST)**		
II. Date it was signed/launched	**2019**	**III. Link**	**https://www.first.org/global/sigs/ethics/ethics-first-20191202.pdf**
IV. Stakeholder groups party to the agreement	**Multistakeholder**	**V. Total Signatories/supporters**	**598**
VI. Organization responsible for ongoing management of agreement (if any)	**FIRST**		

Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Pg. 3	*"Team members should be aware that their actions may impact human rights of others, by sharing information, possible bias in their actions, or by infringing property rights."*
	1.2 Personal data	Pg. 3	*"Data collection is necessary for incident response, but a balance should be struck between the goal of incident response and respecting the data stakeholders. During an investigation, the amount of*

			information needed to collect may change. While progressing through an incident, team members should adjust what they are collecting as the need changes."
2. Information security and resilience measures	**2.1 CIP**	Pg. 3	*"Teams have a responsibility to be able to continue to provide the services they have promised to provide to their constituents."*
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	Pg. 4	*"Before sharing data with third parties for mitigation, the risks should be gauged against the benefits. Data should only be shared if the benefit clearly outweighs the risks. Sensitive data should be stored so that it can easily be destroyed after an incident has been closed. Collected data should be safely destroyed in accordance with data retention policies."*
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	Pg. 2	*"Team members who learn of a vulnerability should follow coordinated vulnerability disclosure by cooperating with stakeholders to remediate the security vulnerability and minimize harm associated with disclosure. Stakeholders include but are not limited to the vulnerability reporter, affected vendor(s), coordinators, defenders, and downstream customers, partners and users."*
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 2	*"Duty to Acknowledge: Team members should respond to inquiries in a timely manner, even if it is only to confirm that the request has been received."*

	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	Pg. 4	*"Teams should operate on the basis of verifiable facts. When sharing information, such as indicators of compromise (IOCs) or incident descriptions, Team members should provide evidence and scope transparently. If this is not possible, the reasons for not sharing this evidence and scope should be given with the information."*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	Pg. 3	*"Team members should be aware that their actions may impact human rights of others, by sharing information, possible bias in their actions, or by infringing property rights. Team members have access to a wide range of personal, sensitive and confidential information in the course of handling incidents. This information should be handled in a way to uphold human rights."*
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	Pg. 3	*"Team members should recognize and respect the jurisdictional boundaries, legal rights, rules, and authorities of the parties involved in incident response related activities. National CSIRTs may have designated responsibilities and/or authority for activities involving constituents within their own jurisdiction, and they may also collaborate with or "hand off" information and activities to other entities that have authority for jurisdictions that cross boundaries."*
	5.8 Internet	N/A	

	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	Pg. 2	*"Team members need to be aware of how their actions may affect their constituents, and ensure they do not cause additional harm while performing their duties. Possible consequences of these actions should be explained to the affected stakeholders."*
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description: Duty to Maintain Confidentiality and Duty to Inform***	Pg. 2	*"Duty to Maintain Confidentiality: Team members have a duty to maintain confidentiality where appropriate. Duty to Inform: Team members should consider it their duty to keep their constituents informed about current security threats and risks. When Team members have information that can either adversely affect or improve safety and security, they have a duty to inform relevant parties or others who can help, with appropriate effort, while duly considering confidentiality, privacy laws and regulations, or other obligations."*

xiv. Freedom Online Coalition Joint Statement on the Human Rights of Cybersecurity Laws, Policies, and Practices

Agreement Overview			
I. Name of Agreement	**FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies**		
II. Date it was signed/launched	**Friday 7 February 2020**	**III. Link**	**https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf**
IV. Stakeholder groups party to the agreement	**Government**	**V. Total Signatories/supporters**	**31 (in 2020)**
VI. Organization responsible for ongoing	**Digital Defenders Partnership (https://www.digitaldefenders.org/)**		

management of agreement (if any)	

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	P5, Para. 14	*“States need to comply with their obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation.”*
		P5. Para. 20	*“As humans are directly impacted by potential threats in cyberspace, including cyberattacks, due attention should be paid to the human dimension of cybersecurity. This includes direct and indirect harm to individual well-being manifesting itself in a range of ways including loss of life, loss of access to vital services, financial loss, undermining of democratic institutions and processes, suppression of the rights to freedom of expression and freedom of association, and failure to respect the right to be free from arbitrary or unlawful interference with privacy, etc”*
	1.2 Personal data		
2. Information security and resilience measures	**2.1 CIP**		
	2.2 Essential services	P5. Para. 15	*“States need to develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law, and seek to minimise potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists.”*

	2.3 Electoral processes		
	2.4 Public trust	P2-3, Para. 4	*"The purpose of this statement is to reaffirm and build on the 2016 commitments while elaborating further on the human rights based approach to cyber security as a basis for strengthening cybersecurity, promoting stability in cyberspace, and promoting emerging technologies that are trust-worthy whilst ensuring the protection of all online users"*
	2.5 Computer emergency response		
	2.6 Incident mitigation		
	2.7 Cyber hygiene	P6, Para. 24	*"States should encourage private sector actors to promote and practice good cyber hygiene"*
3. Reliability of products	**3.1 Supply chain**	P4, Para. 12	*"The FOC also acknowledges that the risks that some technologies and practices pose to the enjoyment of human rights can be exacerbated when governments seek to compel the suppliers of such technologies to cooperate with their security and intelligence agencies without any democratic or independent checks or balances on these authorities"*
	3.2 Reporting of vulnerabilities		
4. Cooperation and assistance	**4.1 General cooperation**	P3, Para. 8	*"Promoting stability of cyberspace is not the responsibility of States alone. A number of multistakeholder initiatives recognise the important role of other actors including industry, civil society, the technical community and academia. The private sector also plays a critical role in creating and maintaining digital services and infrastructure as well as introducing innovative initiatives promoting cybersecurity leadership."*

		P5, Para. 17	*"States should promote international cooperation on cyber issues that focuses on protecting and upholding human rights in order to build mutual trust between all stakeholders."*
	4.2 Law enforcement assistance	P4,Para. 11	*"While State authorities are responsible for protecting the human rights of those in their territory and law enforcement should be enabled to assist victims of harmful cyber activities,"*
	4.3 CIP assistance		
	4.4 Due diligence	P4. Para. 12	*"The FOC also notes the challenges posed to business and government alike by the scarcity of domestic laws, international best practice, and private sector awareness of human rights abuses linked to the export of items with surveillance capabilities and tools to support efforts to conduct human rights due diligence to mitigate the risk of potential adverse human rights impacts."*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**		
	5.2 Intellectual property		
	5.3 Non-proliferation		
	5.4 Non-state actors		
	5.5 Botnets		
	5.6 CIP		
	5.7 CERTs/CSIRTs		
	5.8 Internet		

	5.9 Election infrastructure		
	5.10 Harmful hidden functions		
6. Technical/Operational	**6.1 Network Security Practices**	P6, Para. 22	*"States should encourage private sector actors to adhere to the UN Guiding Principles on Business and Human Rights, to improve their accountability and to share best practices in this respect and help to share lessons learned."*
Any other norms areas included?	***Description:***		

xv. G20 Leaders Communique

Agreement Overview			
I. Name of Agreement	**G20 Leaders Communique**		
II. Date it was signed/launched	**15-16 November 2015**	**III. Link**	http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/
IV. Stakeholder groups party to the agreement	**Governments.**	**V. Total Signatories/supporters**	**20**
VI. Organization responsible for ongoing management of agreement (if any)	**The OECD is a Strategic Partner to the G20 and performs a de facto role as Secretariat for the Group.**		

Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**

1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	Para. 26	*“All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.”*
2. Information security and resilience measures	**2.1 CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	Para. 26	*“We acknowledge that threats to the security of and in the use of ICTs, risk undermining our collective ability to use the Internet to bolster economic growth and development around the world.”*
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Para. 26	*“In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations.”*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	

5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	Para. 26	*“we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors/”*
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	Para. 26	*“In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations.”*
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	Para. 26	*“We commit ourselves to bridge the digital divide.”*

xvi. G7 declaration on responsible state behaviour in cyberspace

Agreement Overview	
I. Name of Agreement	**G7 declaration on responsible state behaviour in cyberspace**

II. Date it was signed/launched	**11 April 2017**	**III. Link**	**https://www.mofa.go.jp/files/000246367.pdf**
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**7**
VI. Organization responsible for ongoing management of agreement (if any)	**G7 presidency (rotating)**		
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Pg. 2 Norm 5	*"We also reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties;"* *"States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;"*
	1.2 Personal data		
2. Information security and resilience measures	**2.1 CIP**	Norm 7	*"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;"*

	2.2 Essential services		
	2.3 Electoral processes		
	2.4 Public trust		
	2.5 Computer emergency response		
	2.6 Incident mitigation	Norm 8	*"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;"*
	2.7 Cyber hygiene		
3. Reliability of products	**3.1 Supply chain**	Norm 9	*"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;"*
	3.2 Reporting of vulnerabilities	Norm 10	*"States should encourage responsible reporting 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;"*
4. Cooperation and assistance	**4.1 General cooperation**	Norm 1	*"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;"*
	4.2 Law enforcement assistance	Norm 4	*"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;”
	4.3 CIP assistance		
	4.4 Due diligence		
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	Pg. 3 Pg. 3 Norm 3	*“under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law.”* *“States may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace.”* *“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;”*
	5.2 Intellectual property	Norm 12	*“No country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”*
	5.3 Non-proliferation		
	5.4 Non-state actors		
	5.5 Botnets		
	5.6 CIP		
	5.7 CERTs/CSIRTs	Norm 6	*“States should not conduct or 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 5 not use authorized emergency response teams to engage in malicious international activity.”
	5.8 Internet		
	5.9 Election infrastructure		
	5.10 Harmful hidden functions		
6. Technical/Operational	**6.1 Network Security Practices**		
Any other norms areas included?	***Description:*** ***National efforts to combat cybercrime (additional item under area #2?)***	Norm 3	*“States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;”*
	Perform due diligence exercise constraint when attributing cyber incidents to another state (additional item under area #5)?	Norm 2	*“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;”*

xvii. GCSC’s Six Critical Norms

Agreement Overview			
I. Name of Agreement	**GCSC’s Six Critical Norms**		
II. Date it was signed/launched	**November 2019**	**III. Link**	**https://cyberstability.org/norms/#toggle-id-2**
IV. Stakeholder groups party to the agreement	**Multistakeholder**	**V. Total Signatories/supporters**	**N/A**

VI. Organization responsible for ongoing management of agreement (if any)	**Global Commission on the Stability of Cyberspace (GCSC)/ The Hague Centre for Strategic Studies**

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	N/A	**NOTE: The six norms do not contain references to human rights, but the norms are accompanied by four principles, one of which is human rights.**
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP**	N/A	**NOTE: Certain IT products and services are essential to the stability of cyberspace due to their use within the core technical infrastructure, such as in core name resolution or routing, because of their widespread facilitation of the user Internet experience, or their criticality to the functioning of critical infrastructures such as election systems or power generation. 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.**
	2.2 Essential services	N/A	
	2.3 Electoral processes	Art. 2	*"State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites."*
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	

	2.7 Cyber hygiene	Art. 7	*“States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.”*
3. Reliability of products	**3.1 Supply chain**	Art. 3	*“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.”*
	3.2 Reporting of vulnerabilities	Para 39	*“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. Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) 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.”*
4. Cooperation and assistance	**4.1 General cooperation**	N/A	
	4.2 Law enforcement assistance	Para 37	*“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. However, state, and non-state actors should not commandeer civilian devices of the general public (en masse) to facilitate or directly execute offensive cyber operations, irrespective of motivation.”*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	**NOTE: In practice, the cyber battlefield (i.e., cyberspace) is designed, deployed, and operated primarily by the private sector. Governments are, despite their unique responsibilities, not the exclusive protectors of this domain. Even if governments maintain a de jure monopoly over the legitimate use of force in cyberspace, they no longer have a**

			practical monopoly on attacking and protecting this domain, nor can they prevent the proliferation and use of powerful cyber weapons. Rather, the technical community, civil society, and individuals also play a major role in the protection of cyberspace, including the promulgation of standards. Therefore, the multistakeholder approach is necessary to improve outcomes and ensure that the norms and policies supporting the stability of cyberspace are well-formed and avoid unwanted consequences.
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	Art. 8; Para 45	*"Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.* *Responsibilities should be imposed on non-state actors as well, as they must exercise restraint or take affirmative steps to ensure the stability of cyberspace."* **NOTE: The participation of non-state actors in matters affecting the stability of cyberspace is unavoidable. For example, many members of the private sector and technical community may be responsible for critical protocols and services, and they may protect states that use their commercial and open-source products. Additionally, even the investigation and attribution of attacks, a traditional role for and political prerogative of governments, is no longer their sole area of knowledge and responsibility; some notable state attacks have been identified and publicized by non-governmental entities. In short, even though states have a unique role to play during and after an attack (including law enforcement activity and/or taking diplomatic or other state actions), they have no monopoly on investigation and attribution, nor can they effectively exclude non-state actors. As a result, developing successful cyberspace norms and policies—and ensuring adherence to them—requires participation by, and is a responsibility of, all stakeholders, and governments must focus on creating mechanisms that effectively incorporate participation of the**

			private sector, the technical community, academia, and other representatives of civil society.
	5.5 Botnets	Art. 4	*"State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes."*
	5.6 CIP	N/A	N/A
	5.7 CERTs/CSIRTs	N/A	N/A
	5.8 Internet	Art. 1	*"State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace."*
	5.9 Election infrastructure	Art. 2	*"State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites."*
	5.10 Harmful hidden functions	Art. 3	*"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."*
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	N/A	

xviii. ITU-T WTSA Resolution 50 - Cybersecurity

Agreement Overview			
I. Name of Agreement	**ITU-T WTSA Resolution 50 - Cybersecurity**		
II. Date it was signed/launched	**2004**	**III. Link**	https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-E.pdf

IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**ITU Member States**
VI. Organization responsible for ongoing management of agreement (if any)	**International Telecommunication Union**		

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	Pg. 5, Para 7	*"To support the Director of the Telecommunication Development Bureau in assisting Member States in the establishment of an appropriate framework among developing countries allowing rapid response to major incidents, and to propose an action plan to increase their protection, taking into account mechanisms and partnerships, as appropriate;"*
	2.7 Cyber hygiene	N/A	

3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 4, Para 6	*"That global, consistent and interoperable processes for sharing incident-response related information should be promoted;"*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	Pg. 4, Para 3	*"That ITU-T continue to raise awareness, within its mandate and competencies, of the need to harden and defend information and telecommunication systems from cyberthreats and cyberattacks, and continue to promote cooperation among appropriate international and regional organizations in order to enhance exchange of technical*

			information in the field of information and telecommunication network security;"
Any other norms areas included?	**Confidence Building**	Pg. 3, Para 1	*"To continue to give this work high priority within ITU-T, in accordance with its competencies and expertise, including promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at the national regional and international level;"*
		Pg. 4, Para 5	*"That ITU-T continue work on the development and improvement of terms and definitions related to building confidence and security in the use of telecommunications/ICTs, including the term cybersecurity;"*
		Pg. 5, Para 8	*"To support relevant ITU-T study group activities related to strengthening and building confidence and security in the use of ICTs,"*
	Standards	Pg. 4, Para 8	*"That ITU-T study groups continue to liaise with standards organizations and other bodies active in this field;"*
		Pg. 4, Para 9	*"That security aspects are considered throughout the ITU-T standards-development process."*

xix. Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

Agreement Overview			
I. Name of Agreement	**Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU**		
II. Date it was signed/launched	**September 2017**	**III. Link**	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**27**
VI. Organization responsible for ongoing management of agreement (if any)	**European Commission**		
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Sec 4.1 (Pg. 18)	*"A comprehensive approach to cybersecurity requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights Guidelines on online freedom"*
	1.2 Personal data	Sec. 4 (Pg. 18)	*"Guided by the EU core values and fundamental rights such as freedom of expression and the right to privacy and protection of personal data, and the promotion of the open, free and secure cyberspace, the EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber stability, as well as contributing to Europe's strategic autonomy in cyberspace."*
2. Information security and resilience measures	**2.1CIP**	N/A	
	2.2 Essential services	Sec. 2.2 (Pg. 5) Sec. 2.7 (Pg. 11)	*"These priorities should take particular account of the evolving cybersecurity threat landscape, as well as the importance of essential services such as transport, energy, health care, banking, financial market infrastructures, drinking water or digital infrastructure."* *"In addition, public institutions, especially those providing essential services, should ensure that their staff are trained in cybersecurity-related areas."*

	2.3 Electoral processes	Sec. 2.7 (Pg. 12)	*“Awareness-raising in relation to online disinformation campaigns and fake news on social media specifically aimed at undermining democratic processes and European values is equally important. While the primary responsibility remains at national level – including for European Parliament elections – the pooling of expertise and sharing of experience at the European level has proven to be of value-added in providing a focus for action.”*
	2.4 Public trust	Sec. 2.2 (Pg. 5)	*“This could be part of the "duty of care" principle, to be further developed together with the industry, which could reduce product/software vulnerabilities by applying a range of methods from design to testing and verification, including formal verification where applicable, long term maintenance, and the use of secure development lifecycle processes, as well as developing updates and patches to address previously undiscovered vulnerabilities and fast update and repair. This would also increase consumers' trust in digital products.”*
	2.5 Computer emergency response	Sec. 2.21 (Pg. 4)	*“ENISA, in cooperation with the relevant bodies at Member State and EU level, notably the network of Computer security incident response teams17, CERT-EU, Europol and the EU Intelligence and Situation Centre (INTCEN), will also contribute to EU-level situational awareness.”*
	2.6 Incident mitigation		*“When a cyber-attack takes place, a fast and effective response can mitigate its impact. This can also demonstrate that public authorities are not powerless in the face of cyber-attacks, and contribute to building trust. As regards the EU institutions' own response, in the first instance the cyber aspects should be mainstreamed into existing EU crisis management mechanisms: the EU integrated political crisis response, coordinated by the Presidency of the Council and the EU's general rapid alert systems. The need to respond to a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause.”*
	2.7 Cyber hygiene	Sec. 2.7	*“People need to develop cyber hygiene habits and businesses and organisations must adopt appropriate risk-based cybersecurity*

		(Pg. 11)	*programmes and update them regularly to reflect the evolving risk landscape.”*
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	Sec. 2.2 (Pg. 6)	*“Furthermore, the important role of third party security researchers in discovering vulnerabilities in existing products and services needs to be acknowledged and conditions to enable coordinated vulnerability disclosure should be created across Member States, building on best practices and relevant standards.”*
4. Cooperation and assistance	**4.1 General cooperation**	Sec. 5 (Pg. 20)	*“This Communication puts forward targeted measures that will further strengthen the EU's cybersecurity structures and capabilities in a coordinated manner, with the full cooperation of the Member States and the different EU structures concerned and respecting their competencies and responsibilities. Its implementation will provide a clear 21 demonstration that the EU and the Member States will work together to put in place a standard of cybersecurity equal to the ever-growing challenges faced by Europe today.”*
	4.2 Law enforcement assistance	Sec. 3.1 (Pg. 13)	*“Europol has become a key actor in supporting Member States' multijurisdictional investigations. It should become a centre of expertise for Member States' law enforcement on online investigations and cyber forensics.”*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	Sec. 4.1 (Pg. 18)	*“On a bilateral level, cyber dialogues85 will be further developed and complemented by efforts to facilitate cooperation with third countries to reinforce principles of due diligence and state responsibility in cyberspace.”*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	

	5.3 Non-proliferation	Sec. 4.1 (Pg. 19)	*"The Commission has also put forward a proposal to modernise EU export controls, including the introduction of controls on the export on critical cyber-surveillance technologies that could cause violations of human rights or be misused against the EU's own security and will step up dialogues with third countries to promote global convergence and responsible behaviour in this area."*
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	N/A	

xx. Mutually Agreed Norms for Routing Security

Agreement Overview			
I. Name of Agreement	**Mutually Agreed Norms for Routing Security**		
II. Date it was signed/launched	**2021**	**III. Link**	https://www.manrs.org/isps/

IV. Stakeholder groups party to the agreement	**Multistakeholder**	**V. Total Signatories/supporters**	**N/A**
VI. Organization responsible for ongoing management of agreement (if any)	**Internet Society**		

Norms Analysis

Category	Norms elements	Paragraph/citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	Pg. 8	*"The MANRS Secretariat may request a response from a network operator within 24 hours of becoming aware of a routing incident, and may also issue a public statement…"*
	2.6 Incident mitigation	Pg. 8	*"The MANRS Secretariat will initially attempt to contact a network operator through its registered MANRS representative(s). If these contacts are no longer valid or there is no response within 72 hours, the MANRS Secretariat will subsequently attempt to contact the technical or abuse contact registered in the appropriate RIR (or NIR) database and/or in PeeringDB."*

	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 1	*"Promote a culture of collective responsibility towards the security and resilience of the Internet's global routing system"*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	Pg. 8	*"A network operator must take steps to identify and mitigate any routing incident originating from either their ASN(s) or a direct customer ASN within 24 hours of becoming aware or being notified of an incident. Within 72 hours, they must also notify the MANRS Secretariat <manrs@isoc.org> of any routing incident where this has caused noticeable disruption to the global routing system, indicating the mitigation measures that are being or have been taken. The MANRS Secretariat may then disseminate this information to the other MANRS Participants."*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	

	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	Pg. 5	*"A network operator should implement a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network."*
Any other norms areas included?	***Description:***		

xxi. NATO Cyber Defense Pledge

Agreement Overview			
I. Name of Agreement	**The NATO Cyber Defence Pledge**		
II. Date it was signed/launched	**08 July 2016**	**III. Link**	**https://www.nato.int/cps/en/natohq/official_texts_133177.htm**
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**30**
VI. Organization responsible for ongoing management of agreement (if any)	**North Atlantic Treaty Organization**		

Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**

1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP**	N/A	
	2.2 Essential services	Sec. 5.I	*"We will...Develop the fullest range of capabilities to defend our national infrastructures and networks."*
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	Sec 5.V	*"Enhance skills and awareness***,** *among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;"*
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	5.IV	*"We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales."* *"We emphasise NATO's role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled."*

			“We will...Improve our understanding of cyber threats, including the sharing of information and assessments;” *“We will...Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen cooperation and the exchange of best practices”*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	Sec. 3	*“We recognise the value of NATO’s partnerships with partner nations, industry and academia, including through the NATO Industry Cyber Partnership”*
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	

Any other norms areas included?	***Description:***		

xxii. Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021)

Agreement Overview			
I. Name of Agreement	**Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021)**		
II. Date it was signed/launched	**March 12, 2021**	**III. Link**	https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**193**
VI. Organization responsible for ongoing management of agreement (if any)	**International Organization: United Nations**		
Norms Analysis			
Category	**Norms elements**	**Paragraph /citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Para. 15	*"States concluded that they are increasingly concerned about the implications of the malicious use of ICTs for the maintenance of international peace and security, and subsequently for human rights*

			and development. In particular, concern was expressed regarding the development of ICT capabilities for purposes that undermine international peace and security. Harmful ICT incidents are increasing in frequency and sophistication and are constantly evolving and diversifying. Increasing connectivity and reliance on ICTs without accompanying measures to ensure ICT security can bring unintended risks, making societies more vulnerable to malicious ICT activities. Despite the invaluable benefits of ICTs for humanity, their malicious use can have significant and far-reaching negative impacts."
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	Para. 31	*"States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore, States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection."*
	2.2 Essential services	Para. 26	*"While agreeing on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, along with endeavouring to ensure the general availability and integrity of the Internet, States further concluded that the COVID19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure. such as those affirmed by consensus through UN General Assembly resolution 70/237."*
	2.3 Electoral processes	Para. 18	*"States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. While it is each State's prerogative to determine which infrastructures it*

			designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation. Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability."
	2.4 Public trust	N/A	
	2.5 Computer emergency response	Para. 46	*"Drawing from the lessons and practices shared at the OEWG, States concluded that the prior existence of national and regional mechanisms and structures, as well as the building of adequate resources and capacities, such as national Computer Emergency Response Teams (CERTs), are essential to ensuring that CBMs serve their intended purpose."*
	2.6 Incident mitigation	Para. 54	*"The international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. It is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. Capacity-building helps to develop the skills, human resources, policies, and institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies. It plays an important enabling function for promoting adherence to international law and the implementation of norms of responsible State behaviour, as well as supporting the implementation of CBMs. In a digitally interdependent world, the benefits of capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all."*

	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	Para. 28	*"States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities."*
	3.2 Reporting of vulnerabilities	Para. 28	*"States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities."*
4. Cooperation and assistance	**4.1 General cooperation**	Para. 55	*"Ensuring an open, secure, stable, accessible and peaceful ICT environment requires effective cooperation among States to reduce risks to international peace and security. Capacity-building is an important aspect of such cooperation and a voluntary act of both the donor and the recipient."*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	Para. 54	*"The international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. It is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. Capacity-building helps to develop the skills, human resources, policies, and institutions that increase the resilience and security of States so they can fully enjoy the*

			benefits of digital technologies. It plays an important enabling function for promoting adherence to international law and the implementation of norms of responsible State behaviour, as well as supporting the implementation of CBMs. In a digitally interdependent world, the benefits of capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all."
	4.4 Due diligence	Para. 31	*"States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore, States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection."*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	Para. 16	*"States recalled that a number of States are developing ICT capabilities for military purposes. They also recalled that the use of ICTs in future conflicts between States is becoming more likely. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States."*
	5.5 Botnets	N/A	
	5.6 CIP	Para. 31	*"States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore,*

			States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection."
	5.7 CERTs/CSIRTs	Para. 61	*"States recalled the need for a concrete, action-oriented approach to capacity-building. States concluded that such concrete measures could include support at both the policy and technical levels such as the development of national cyber security strategies, providing access to relevant technologies, support to Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) and establishing specialized training and tailored curricula including "training the trainer" programmes and professional certification. The benefits of establishing platforms for information exchange including legal and administrative good practices was recognized, as were the valuable contributions of other relevant stakeholders to capacity-building activities."*
	5.8 Internet	N/A	
	5.9 Election infrastructure	Para. 18	*"States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. While it is each State's prerogative to determine which infrastructures it designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation. Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability."*

	5.10 Harmful hidden functions	Para. 28	*"States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities."*
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description: Capacity Building, Confidence Building***	Para. 41-47; Para. 54-56	*"Confidence-building measures (CBMs), which comprise transparency, cooperative and stability measures can contribute to preventing conflicts, avoiding misperception and misunderstandings, and the reduction of tensions. They are a concrete expression of international cooperation. With the necessary resources, capacities and engagement, CBMs can strengthen the overall security, resilience and peaceful use of ICTs. CBMs can also support implementation of norms of responsible State behaviour, in that they foster trust and ensure greater clarity, predictability and stability in the use of ICTs by States. Together with the other pillars of the framework for responsible State behaviour, CBMs can also help build common understandings among States, thereby contributing to a more peaceful international environment."* *"The international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. It is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. Capacity-building helps to develop the skills, human resources, policies, and institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies. It plays an important enabling function*

			for promoting adherence to international law and the implementation of norms of responsible State behaviour, as well as supporting the implementation of CBMs. In a digitally interdependent world, the benefits of capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all."

xxiii. Organization of American States List of Confidence- and Security-Building Measures (CSBMS), Committee on Hemispheric Security

Agreement Overview			
I. Name of Agreement	**Organization of American States List of Confidence and Security-Building Measures (CSBMS), Committee on Hemispheric Security**		
II. Date it was signed/launched	**2020**	**III. Link**	https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/Multilateral/OAS+List+of+Confidence-+and+Security-Building+Measures+%28CSBMs%29.pdf
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**35**
VI. Organization responsible for ongoing management of agreement (if any)	**Organization of American States (OAS)**		
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**

1. Rights and freedoms	**1.1 Human Rights**	Para 25	*“Exchange information related to adopting and adapting provisions under domestic laws that govern processes for obtaining data and information, and exchange experiences involving government, service providers, end users and others, regarding the prevention, management of, and protection against cyber threats, with a view to sustained mutual cooperation to prevent, address, and investigate criminal activities that threaten security and to ensure an open, interoperable, secure and reliable internet, while respecting obligations and commitments under international law and international human rights law in particular.”*
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	Para 24	*“Establish national points of contact regarding natural disaster response, environmental security, transportation security, and critical infrastructure protection.”*
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Para 31	*“To foster cooperation and exchange of best practices on cyber diplomacy, cybersecurity and cyberspace, through, for example, the establishment of working groups, other dialogue mechanisms, and the signing of agreements among states.”*

	4.2 Law enforcement assistance	Para 27	*"Identify a national point of contact at the policy level able to discuss the implications of hemispheric cyber threats. The work of these national points of contact may be distinct from, yet supplement the ongoing work of law enforcement and other technical experts in combating cybercrime and responding to cyber incidents of concern."*
	4.3 CIP assistance	Para 24	*"Establish national points of contact regarding natural disaster response, environmental security, transportation security, and critical infrastructure protection."*
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	N/A	

xxiv. OSCE Confidence Building Measures (2013 & 2016)

Agreement Overview

I. Name of Agreement	OSCE Confidence Building Measures (2013 and 2016)		
II. Date it was signed/launched	3rd of December 2013 10th of March 2016	**III. Link**	https://www.osce.org/files/f/documents/d/1/109168.pdf https://www.osce.org/files/f/documents/d/a/227281.pdf
IV. Stakeholder groups party to the agreement	Government	**V. Total Signatories/supporters**	57
VI. Organization responsible for ongoing management of agreement (if any)	Organization for Security and Co-operation in Europe, Transnational Threats Department		

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	2013: Interpretative statement by the Russian Federation	In the 2013 release, the Russian Federation included a reference that it will be guided in its implementation by a firm commitment to the principles of non-interference in the internal affairs of States, their equality in the process of Internet governance and the sovereign right of States to Internet governance in their national information space, to international law and to the **observance of fundamental human rights and freedoms.** “
	1.2 Personal data		
	2.1 CIP		

2. Information security and resilience measures	**2.2 Essential services**		
	2.3 Electoral processes		
	2.4 Public trust		
	2.5 Computer emergency response	2013: CBM 8	*" Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts*. "
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	2013 2013	*"Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties. "* *"Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs*
	4.2 Law enforcement assistance	2013	*"Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs"*
	4.3 CIP assistance	N/A	

	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	2016	*"Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to* ***counter terrorist or criminal use of ICTs****."*
	5.5 Botnets	N/A	
	5.6 CIP	2016 2016:	*"Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;"* *"Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and"*
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	

Any other norms areas included?	***Description:*** ***Interoperability and reliability***	2013	*"Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet"*

xxv. Paris Call for Trust and Security in Cyberspace

Agreement Overview			
I. Name of Agreement	**The Paris Call for Trust and Security in Cyberspace**		
II. Date it was signed/launched	**12th of November, 2018**	**III. Link**	**https://pariscall.international/** **https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf**
IV. Stakeholder groups party to the agreement	**Multistakeholder**	**V. Total Signatories/supporters**	**1200+, including 80 governments**
VI. Organization responsible for ongoing management of agreement (if any)	**French Ministry for Europe and Foreign Affairs**		

Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	(PDF, Para. 4)	*"We reaffirm that the same rights that people have offline must also be protected online, and also reaffirm the applicability of international human rights law in cyberspace."*
	1.2 Personal data		

2. Information security and resilience measures	**2.1 CIP**	PDF, Pg. 2, Principle 1	*“Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;”*
	2.2 Essential services		
	2.3 Electoral processes	PDF Pg. 3, Principle 3	*“Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;”*
	2.4 Public trust		
	2.5 Computer emergency response		
	2.6 Incident mitigation		
	2.7 Cyber hygiene	PDF Pg. 3, Principle 7	*“Support efforts to strengthen an advanced cyber hygiene for all actors”;*
3. Reliability of products	**3.1 Supply chain**	PDF Pg. 3, Principle 6	*“Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain;”*
	3.2 Reporting of vulnerabilities		
4. Cooperation and assistance	**4.1 General cooperation**	PDF Pg. 3, Principle 9	*“Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace”*
	4.2 Law enforcement assistance		
	4.3 CIP assistance		
	4.4 Due diligence		
	5.1 Developing and deploying cyber weapons		

5. Restraint on development and use of cyber capabilities	**5.2 Intellectual property**	PDF Pg. 3, Principle 4	*"Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;"*
	5.3 Non-proliferation		
	5.4 Non-state actors	PDF Pg. 3, Principle 8	*"Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors;"*
	5.5 Botnets		
	5.6 CIP		
	5.7 CERTs/CSIRTs		
	5.8 Internet	PDF Pg. 2, Principle 2	*"Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;"*
	5.9 Election infrastructure		
	5.10 Harmful hidden functions	PDF Pg.3, Principle 5	*"Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;"*
6. Technical/Operational	**6.1 Network Security Practices**		
Any other norms areas included?	***Description:***		

xxvi. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (Joint Communication to the European Parliament and the Council)

Agreement Overview

I. Name of Agreement	Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU		
II. Date it was signed/launched	Sept. 2017	**III. Link**	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en
IV. Stakeholder groups party to the agreement	Governments	**V. Total Signatories/supporters**	27
VI. Organization responsible for ongoing management of agreement (if any)	European Commission		

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	Sec 4.1 (Pg. 18)	*"A comprehensive approach to cybersecurity requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights Guidelines on online freedom"*
	1.2 Personal data	Sec. 4 (Pg. 18)	*"Guided by the EU core values and fundamental rights such as freedom of expression and the right to privacy and protection of personal data, and the promotion of the open, free and secure cyberspace, the EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber stability, as well as contributing to Europe's strategic autonomy in cyberspace."*
2. Information security and resilience measures	**2.1CIP**	N/A	
	2.2 Essential services	Sec. 2.2 (Pg. 5)	*"These priorities should take particular account of the evolving cybersecurity threat landscape, as well as the importance of essential*

		Sec. 2.7 (Pg. 11)	*services such as transport, energy, health care, banking, financial market infrastructures, drinking water or digital infrastructure.”* *“In addition, public institutions, especially those providing essential services, should ensure that their staff are trained in cybersecurity-related areas.”*
	2.3 Electoral processes	Sec. 2.7 (Pg. 12)	*“Awareness-raising in relation to online disinformation campaigns and fake news on social media specifically aimed at undermining democratic processes and European values is equally important. While the primary responsibility remains at national level – including for European Parliament elections – the pooling of expertise and sharing of experience at the European level has proven to be of value-added in providing a focus for action.”*
	2.4 Public trust	Sec. 2.2 (Pg. 5)	*“This could be part of the "duty of care" principle, to be further developed together with the industry, which could reduce product/software vulnerabilities by applying a range of methods from design to testing and verification, including formal verification where applicable, long term maintenance, and the use of secure development lifecycle processes, as well as developing updates and patches to address previously undiscovered vulnerabilities and fast update and repair. This would also increase consumers' trust in digital products.”*
	2.5 Computer emergency response	Sec. 2.21 (Pg. 4)	*“ENISA, in cooperation with the relevant bodies at Member State and EU level, notably the network of Computer security incident response teams17, CERT-EU, Europol and the EU Intelligence and Situation Centre (INTCEN), will also contribute to EU-level situational awareness.”*
	2.6 Incident mitigation		*“When a cyber-attack takes place, a fast and effective response can mitigate its impact. This can also demonstrate that public authorities are not powerless in the face of cyber-attacks, and contribute to building trust. As regards the EU institutions' own response, in the first instance the cyber aspects should be mainstreamed into existing EU*

			crisis management mechanisms: the EU integrated political crisis response, coordinated by the Presidency of the Council and the EU's general rapid alert systems. The need to respond to a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause.”
	2.7 Cyber hygiene	Sec. 2.7 (Pg. 11)	*“People need to develop cyber hygiene habits and businesses and organisations must adopt appropriate risk-based cybersecurity programmes and update them regularly to reflect the evolving risk landscape.”*
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	Sec. 2.2 (Pg. 6)	*“Furthermore, the important role of third party security researchers in discovering vulnerabilities in existing products and services needs to be acknowledged and conditions to enable coordinated vulnerability disclosure should be created across Member States, building on best practices and relevant standards.”*
4. Cooperation and assistance	**4.1 General cooperation**	Sec. 5 (Pg. 20)	*“This Communication puts forward targeted measures that will further strengthen the EU's cybersecurity structures and capabilities in a coordinated manner, with the full cooperation of the Member States and the different EU structures concerned and respecting their competencies and responsibilities. Its implementation will provide a clear 21 demonstration that the EU and the Member States will work together to put in place a standard of cybersecurity equal to the ever-growing challenges faced by Europe today.”*
	4.2 Law enforcement assistance	Sec. 3.1 (Pg. 13)	*“Europol has become a key actor in supporting Member States' multijurisdictional investigations. It should become a centre of expertise for Member States' law enforcement on online investigations and cyber forensics.”*
	4.3 CIP assistance	N/A	

	4.4 Due diligence	Sec. 4.1 (Pg. 18)	*"On a bilateral level, cyber dialogues85 will be further developed and complemented by efforts to facilitate cooperation with third countries to reinforce principles of due diligence and state responsibility in cyberspace."*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	Sec. 4.1 (Pg. 19)	*"The Commission has also put forward a proposal to modernise EU export controls, including the introduction of controls on the export on critical cyber-surveillance technologies that could cause violations of human rights or be misused against the EU's own security and will step up dialogues with third countries to promote global convergence and responsible behaviour in this area."*
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***		

xxvii. Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security

Agreement Overview			
I. Name of Agreement	**Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security**		
II. Date it was signed/launched	**Ekaterinburg, 16 June 2009**	**III. Link**	**http://eng.sectsco.org/load/207508/**
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**6 Member States of SCO** **China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan**
VI. Organization responsible for ongoing management of agreement (if any)	**The Shanghai Cooperation Organisation**		
Norms Analysis			
Category	**Norms elements**	**Paragraph/citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	

	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	

4. Cooperation and assistance	**4.1 General cooperation**	Art. 3 Major Areas of Cooperation	*1) defining, coordinating and implementing necessary joint measures in the field of ensuring international information security;* *2) creating of a system of joint monitoring and response to emerging threats in this area;* *3) elaborating joint measures for the development of the provisions of the international law limiting the spread and use of information weapons threatening defense capacity, national security and public safety;* *4) countering threats related to the use of information and communication technologies for terrorist purposes;* *5) combating cybercrime;* *6) conducting expertise, research and evaluation in the field of information security necessary for the purposes of this Agreement;* *7) promoting secure, stable operation and governance internationalization of the global Internet network;* *8) ensuring information security of the critically significant structures of the Parties;* *9) developing and implementing joint measures of trust conducive to ensuring international information security;* *10) developing and implementing coherent policies and organizational and technical procedures for the implementation of digital signature and data protection in the cross-border exchange of information;* *11) exchanging information on the legislation of the Parties on issues of information security;* *12) improving the international legal framework and practical mechanisms of cooperation of the Parties in ensuring international information security;* *13) creating conditions for cooperation between the competent authorities of the Parties in order to implement this Agreement;* *14) interacting within international organizations and fora on issues of international information security;* *15) exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums of authorized*

			representatives and experts of the Parties in the field of information security; *16) exchanging information on issues related to the cooperation in the basic areas listed in this Article.*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	Annex 2 List of basic types, sources, and features of threats in the field of International Information Security	*"Development and application of information weapons, preparation and conduct of information warfare.* *The source of this threat is the creation and development of information weapons posing a direct threat to critically important structures of states that may lead to a new arms race and is the main threat in the field of international information security.* *Its features include using information weapons for the purpose of preparing and conducting information warfare, as well as of affecting the systems of transportation, communications, and command of air, ballistic missile and other types of defense facilities resulting in a state losing the ability to defend itself in the face of the aggressor and failing to use its legitimate right of self-defense; disrupting the functioning of the information infrastructure facilities resulting in paralyzed governance and decision-making systems of states; destructively impacting critically important structures."*
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	

	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	The Shanghai Cooperation agreement establishes cooperation proceeding from the presence of threats. Below is the definition of terms as defined in the agreement.	Article 2 Major Threats in the Field of International Information Security	*"In the course of cooperation under this Agreement, the Parties proceed from the presence of the following key threats to international information security:* *1) Developing and using information weapons, preparing and conducting information warfare;* *2) Information terrorism;* *3) Cybercrime;* *4) Use of a dominant position in the information space to the detriment of the interests and security of other States;* *5) Dissemination of information prejudicial to the socio-political and socio- economic systems, spiritual, moral and cultural environment of other States;* *6) Threats to secure and stable functioning of global and national information infrastructures that are natural and/or manmade."*
	Information war	Annex 1 List of Basic Terms in the Field of International Information Security	*"'Information war' means a confrontation between two or more states in the information space with the aim of damaging information systems, processes and resources, critically important and other structures, undermining political, economic and social systems, psychologically manipulating masses of the population to destabilize society and the State, and also forcing the state to take decisions in the interest of the opposing party;"*
	Information terrorism	Annex 1	*"'Information terrorism' means using information resources in the information space and/or influencing on them for terrorist purposes;"*

	Information infrastructure	Annex 1	*"’Information Infrastructure’ means a range of technical tools and systems for formation, generation, transformation, transmission, use and storage of information;”*
	Critical important structures	Annex 1	*"’Critically important structures’ means facilities, systems and institutions of the state, the impact on which may have consequences directly affecting national security, including the security of an individual, society and the state;”*
	Cybercrime	Annex 1	*“‘Cybercrime means using information resources and/or influencing them in the information space for illegal purposes;”*
		Annex 2	*1. Cybercrime.* *“This threat is caused by individuals or organizations engaged in the illegal use of information resources or unwarranted interference with such resources for criminal purposes. Its features include entering into information systems for compromising the integrity, availability and confidentiality of information; intentionally producing and distributing computer viruses and other malicious programs; implementing DOS-attacks (denial of Service) and other negative impacts; damaging information resources; violating legal rights and freedoms of citizens in the field of information, including intellectual property rights and privacy; using information resources and methods to commit crimes such as fraud, embezzlement, extortion, smuggling, drug trafficking, child pornography, etc.”*
	Misuse of information resources	Annex 1	*"’Misuse of information resources’ means using information resources without appropriate rights or in violation of the established rules, the laws of the Parties or the norms of the international law;”*

xxviii. Siemens Charter of Trust

Agreement Overview			
I. Name of Agreement	**Charter of Trust (formerly Siemens Charter of Trust)**		
II. Date it was signed/launched	**2018**	**III. Link**	https://assets.new.siemens.com/siemens/assets/api/uuid:9bbe02e9-fcb2-4948-9977-a668cac52e50/version:1567432347/charter-of-trust-presentation-en-20190902-website.pdf https://www.charteroftrust.com
IV. Stakeholder groups party to the agreement	**Industry**	**V. Total Signatories/supporters**	**13+**
VI. Organization responsible for ongoing management of agreement (if any)	**Siemens**		

Norms Analysis

Category	Norms elements	Paragraph/citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	Pg. 3, Para 2	*2 Security by default* *“Adopt the highest appropriate level of security and data protection and ensure that it's preconfigured into the design of products, functionalities, processes, technologies, operations, architectures and business models.”*

2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	Pg. 6, Paras 7-8	*7 Certification for critical infrastructure and solutions* *“Companies and - if necessary - governments establish mandatory independent third-party certifications {based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions.”* *8 Transparency and response* *“Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice which is focusing on critical infrastructure.”*
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	Pg. 6, Para 2	*2 Responsibility throughout the digital supply chain* *“Companies and - if necessary - governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards, such as:*

			• *Identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.* • *Encryption: Connected devices must ensure confidentiality for data storage and transmission purposes wherever appropriate.* • *Continuous protection: Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism.”*
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 6, Paras 9-10	*9 Regulatory framework* *“Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of the WTO; inclusion of rules for cybersecurity into Free Trade Agreements {FTAs)”* *10 Joint initiatives* *“Drive joint initiatives including all relevant stakeholders, in order to implement the above principles in the various parts of the digital world without undue delay.”*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	

	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	Pg. 6, Paras 1; 3- 4	*1 Ownership of cyber and IT security* *“Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – ‘It is everyone's task’.”* *3 Security by default* *“Adopt the highest appropriate level of security and data protection and ensure that it's preconfigured into the design of products, functionalities, processes, technologies, operations, architectures and business models.”* *4 User-centricity* *“Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks.”*

Any other norms areas included?	**Awareness and education**	Pg. 6, Paras 5-6	*5 Innovation and co-creation* *“Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.e., contractual Public Private Partnerships.”* *6 Education* *“Include dedicated cybersecurity courses in school curricula - as degree courses in universities, professional education and trainings - in order to lead the transformation of skills and job profiles needed for the future.”*

xxix. Southern African Development Community (SADC) Model Law

Agreement Overview			
I. Name of Agreement	Southern African Development Community (SADC) Model Law		
II. Date it was signed/launched	Adopted by SADC ICT Ministers in Mauritius from 6-8 November, 2012	**III. Link**	https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_cybercrime.pdf
IV. Stakeholder groups party to the agreement	Government	**V. Total Signatories/supporters**	This is not a signed agreement, but adopted by SADC ICT ministers and some modeled their laws after this example.
VI. Organization responsible for ongoing	South African Development Community		

management of agreement (if any)			
	Norms Analysis		
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	N/A	
	4.2 Law enforcement assistance	Pg. 15	*"If a [law enforcement] [police] officer that is undertaking a search based on Sec. 25 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system."*

			"Any person, who is not a suspect of a crime or otherwise excluded from an obligation to follow such order, but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 26 must permit, and assist if reasonably required and requested by the person authorized to make the search"...
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	Pg. 1	*"Critical infrastructure means computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters."*
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	Pg. 19, Sec. VI	*"When providing the services contemplated in this Chapter there is no general obligation on an Internet service provider to monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity."*

	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***	Throughout	Generally speaking this document describes what is malicious internet behavior. It is a model law that is picked up by others but does not directly have the force of law.

xxx. The Council to Secure the Digital Economy International Anti-Botnet guide

Agreement Overview			
I. Name of Agreement	**The Council to Secure the Digital Economy International Anti-Botnet guide**		
II. Date it was signed/launched	**2018**	**III. Link**	**https://securingdigitaleconomy.org/wp-content/uploads/2018/11/CSDE-Anti-Botnet-Report-final.pdf**
IV. Stakeholder groups party to the agreement	**Industry**	**V. Total Signatories/supporters**	**17**
VI. Organization responsible for ongoing management of agreement (if any)			
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**

1. Rights and freedoms	**1.1 Human Rights**	N/A	
	1.2 Personal data	Pg. 28	*"Baseline Practices: Device manufacturers may provide notice to the consumer about security support policy and how the device is supported with updates during and what to expect after the support period. Where possible, the device should support network asset management by enabling the ability to identify and audit the device logically and physically and with proper access control. After the support period, consumers should have the ability to, and be informed about, how to "decommission" the device. Decommissioning should allow a consumer to return the product to factory defaults and remove any Personally Identifiable Information (PII)."*
2. Information security and resilience measures	**2.1 CIP** (Critical Infrastructure Protection)	Pg. 13	*"For purposes of this Guide, "infrastructure" refers to all systems that enable connectivity and operability — not just to the physical facilities of providers of internet service, backbone, cloud, web hosting, content delivery, Domain Name System, and other services, but also software-defined networks and other systems that reflect the internet's evolution from tangible things to a digital concept. We recommend baseline practices and advanced capabilities for diverse infrastructure in the modern internet and communications ecosystem."*
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	Pg. 32	*"Summary of Baseline Mitigation Practices: Providers should use ingress filtering — that is, apply a filter that can limit the rate of*

			inbound traffic. Providers should also make a reasonable effort to shape traffic on their networks and use blackholing and sinkholing as network management tools. Summary of Advanced Mitigation Capabilities: Companies with access to greater resources may use egress filtering in addition to ingress filtering, thereby limiting the rate of both outbound and inbound traffic. They may use access control lists (ACLs) to reduce attack vectors. Companies may take steps to minimize service disruptions when shaping traffic, for example by deploying selective black holes. They may use technologies such as BGP flowspec to increase traffic management options. They are able to work in partnership with government and industry to take down malicious botnets. They may also offer commercial services such as scrubbing traffic and DDoS protection."
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	Pg. 28	*"Providers should create a security vulnerability policy and process to identify, mitigate, and where appropriate disclose known security vulnerabilities in their products."*
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 21	*"Baseline Practices: Providers should notify customers or peers who violate the acceptable use policy or engage in nefarious activities. If traffic from a customer or peer is blocked, provide both (1) a text or phone message and (2) email/user account webpage notice. The customer or peer should be provided with clear instructions on how to contact the provider via communications channels that are not being blocked. Advanced Capabilities: Providers with trained staff and dedicated resources can greatly reduce the false positive rate so that customers*

			rarely experience interruption when using services in a legitimate manner.”
	4.2 Law enforcement assistance	Pg. 22	*“Baseline Practices: Providers should maintain an easy-to-find list of points of contact for law enforcement and security researchers. Providers should also have a well-defined policy describing how they can and cannot support law enforcement efforts. Advanced Capabilities: Generally, industry leaders will have more procedures and technologies with which to support law enforcement. They will also have defined policies and legal positions on specific law enforcement tactics. They may conduct global risk assessment to account for global legal requirements. In addition to cooperating with law enforcement, providers may have processes for collaborating with competitors during exceptional events.”*
	4.3 CIP assistance	Pg. 23	*“Baseline Practices: Secure-by-design development should include the following at a minimum: Software security awareness and education: Awareness-raising should extend to all personnel who are part of the software development process, including developers, product managers and others. Cost-effective educational opportunities or training exercises should be made available.”*
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	Pg. 33	*“Enterprises of all sizes also can take their own proactive steps to mitigate ecosystem risk through, for example, implementing appropriate identity and access management techniques and discontinuing the use of legacy and pirated products and*

			software that do not receive updates, among other things. Steps like these can help enterprises protect sensitive data and intellectual property on their networks, in addition to helping to protect the ecosystem at large by reducing the attack surface for DDoS and other distributed attacks."
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	Pg. 15	*"CSDE members take critical steps to increase the resilience of their own networks, their customers' networks, and the global ecosystem against botnets. Experts in government and industry have observed that because of the complexity of the ecosystem, no single tool will always be effective to mitigate threats,37 which means that industry must retain enough flexibility to adapt to emerging threats and new technologies and tools."*
	5.6 CIP	Pg. 23	*"Baseline Practices: Secure-by-design development should include the following at a minimum: Principle of least privilege: By limiting user and application access to only the essential privileges needed to perform necessary tasks, software developers can reduce the attack surface of a product. Applying the principle of least privilege in the design phase reduces the chance that a malicious actor or compromised service will gain administrative access and control over a system."*
	5.7 CERTs/CSIRTs	Pg. 34	*"Enterprises should be prepared to receive and act responsively and responsibly upon cyber threat information provided by information sharing activities even when not yet committed to actively share information. Examples include information from government and law enforcement information sharing activities, various CERTs, industry groups, network providers, RFC2142*

			addresses, and updates and alerts from vendors and other sources."
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	Pg. 29	*"Baseline Practices: If a password is not unique to the device, the installer should change to a strong password. (See [1], 'Passwords'). Different passwords must be used for all devices and systems. The installation should use a trusted password management system. Advanced Capabilities: Multi-factor authentication user access control is used."*
Any other norms areas included?	***Description:***	N/A	

xxxi. The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security

Agreement Overview			
I. Name of Agreement	**The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security**		
II. Date it was signed/launched	**17 October 2016**	**III. Link**	● https://freedomonlinecoalition.com/wg1-launches-recommendations-on-human-rights-based-approaches-to-cybersecurity/ ● https://freeandsecure.online/recommendations/
IV. Stakeholder groups party to the agreement	**Multistakeholder**	**V. Total Signatories/supporters**	30+ countries, 26 organizations, 9 individuals

VI. Organization responsible for ongoing management of agreement (if any)	**Internet Free & Secure Team:** https://freeandsecure.online/about/ **Contact form:** https://freeandsecure.online/contact-us/

Norms Analysis

Category	Norms elements	Paragraph/citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	Recommendations by #	*1.Cybersecurity policies and decision-making processes should protect and respect human rights.* *2.The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.* *5.Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.* *8.Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy.* *9.Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.*
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP**	Recommendations by #	*7. Cybersecurity-related laws, policies and practices should uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services.*

	2.2 Essential services	Recommendations by #	*3. Cybersecurity-related laws, policies and practices should enhance the security of persons online and offline, taking into consideration the disproportionate threats faced by individuals and groups at risk.*
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	Recommendations by #	*6. Responses to cyber incidents should not violate human rights.*
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	*11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.*
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Recommendations by #	*10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.* *12.Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders.*
	4.2 Law enforcement assistance	N/A	
	4.3 CIP assistance	N/A	
	4.4 Due diligence	Recommendations by #	*4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law.*

5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	Sec 1 and all of the recommendations	*These recommendations are a first step towards ensuring that cybersecurity policies and practices are based upon and fully consistent with human rights – effectively, that cybersecurity policies and practices are rights-respecting by design.*
Any other norms areas included?	***Description:***	N/A	

xxxii. UN GGE on advancing responsible State behaviour in cyberspace in the context of international security, final report (2021)

Agreement Overview	
I. Name of Agreement	Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security

II. Date it was signed/launched	28 May 2021	**III. Link**	https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf
IV. Stakeholder groups party to the agreement	Governments	**V. Total Signatories/supporters**	25
VI. Organization responsible for ongoing management of agreement (if any)	United Nations		

Norms Analysis

Category	Norms elements	Paragraph/ citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	Pg.3 para 5 Pg.6 para 36	*"It is in the interest of all and vital to the common good to promote the use of ICTs for peaceful purposes. Respect for sovereignty and human rights and fundamental freedoms, as well as sustainable and digital development remain central to these efforts."* *"Norm 13 (e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression." [from 2015 UN GGE Report]* *"This norm reminds States to respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations."*

	1.2 Personal data	Pg.11 para 58	*“To prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors, States can consider putting in place at the national level:… (b) Legislative and other safeguards that enhance the protection of data and privacy.”*
2. Information security and resilience measures	**2.1CIP**	Pg.9 Pg.9 para 44 Pg.9 para 45	*“Norm 13 (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.” [From 2015 UN GGE report]* *“In this regard, each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure.”* *“The COVID-19 pandemic heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities, including through the implementation of the norms addressing critical infrastructure (such as this norm and norms (g) and (h)). Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet.”*
	2.2 Essential services	Pg.4 para 10 Pg.9 para 45	*“Of specific concern is malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities.”*

			"Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes."
	2.3 Electoral processes	Pg.9 par 45	*"Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes."*
	2.4 Public trust	Pg.11 para 56	"This norm recognizes the need to promote end user confidence and trust in an ICT environment that is open, secure, stable, accessible and peaceful."
	2.5 Computer emergency response	Pg. 12 para 65	*"This norm reflects the fact that CERTs/CSIRTs or other authorized response bodies have unique responsibilities and functions in managing and resolving ICT incidents, and thereby play an important role in contributing to the maintenance of international peace and security. They are essential to effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents. Harm to emergency response teams can undermine trust and hinder their ability to carry out their functions and can have wider, often unforeseen consequences across sectors and potentially for international peace and security. The Group underscores the importance of avoiding the politicization of CERTs/CSIRTs and respecting the independent character of their functions."*
	2.6 Incident mitigation	Pg. 12 para 65	*"This norm reflects the fact that CERTs/CSIRTs or other authorized response bodies have unique responsibilities and functions in managing and resolving ICT incidents, and thereby play an important role in contributing to the maintenance of international peace and security. They are essential to effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents. Harm to*

			emergency response teams can undermine trust and hinder their ability to carry out their functions and can have wider, often unforeseen consequences across sectors and potentially for international peace and security. The Group underscores the importance of avoiding the politicization of CERTs/CSIRTs and respecting the independent character of their functions."
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	Pg. 11 para 56	*"This norm recognizes the need to promote end user confidence and trust in an ICT environment that is open, secure, stable, accessible and peaceful. Ensuring the integrity of the ICT supply chain and the security of ICT products, and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions are increasingly critical in that regard, as well as to international security, and digital and broader economic development."*
	3.2 Reporting of vulnerabilities	Pg. 12 para 60	*"This norm reminds States of the importance of ensuring that ICT vulnerabilities are addressed quickly in order to reduce the possibility of exploitation by malicious actors. Timely discovery and responsible disclosure and reporting of ICT vulnerabilities can prevent harmful or threatening practices, increase trust and confidence, and reduce related threats to international security and stability."*
4. Cooperation and assistance	**4.1 General cooperation**	Pg. 18 para 92	*"States should consider approaching cooperation in ICT security and capacity-building in a manner that is multidisciplinary, multi-stakeholder, modular and measurable."*
	4.2 Law enforcement assistance	Pg. 7para 32	*"Observance of this norm implies the existence of national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs."*

	4.3 CIP assistance	Pg. 10 para 51	*"This norm reminds States that international cooperation, dialogue, and due regard for the sovereignty of all States are central to responding to requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. The norm is particularly important when dealing with those acts that have the potential to threaten international peace and security."*
	4.4 Due diligence	Pg. 6 para 29	*"This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation. It conveys an understanding that a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts."*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	Pg. 5 para 20	*"In this regard, and in furtherance of this norm, the Group encourages States to refrain from using ICTs and ICT networks to carry out activities that can threaten the maintenance of international peace and security."*
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	Pg. 11 para 56	*"Ensuring the integrity of the ICT supply chain and the security of ICT products, and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions are increasingly critical in that regard, as well as to international security, and digital and broader economic development."*
	5.4 Non-state actors	Pg. 14 para 71	*"It also reaffirms that States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."*
	5.5 Botnets	N/A	

	5.6 CIP	Pg. 9	*"Norm 13 (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." [From 2015 UN GGE report]* *"In this regard, each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure."* *"The COVID-19 pandemic heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities, including through the implementation of the norms addressing critical infrastructure (such as this norm and norms (g) and (h)). Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet."*
	5.7 CERTs/CSIRTs	Pg. 12 para 65	*"This norm reflects the fact that CERTs/CSIRTs or other authorized response bodies have unique responsibilities and functions in managing and resolving ICT incidents, and thereby play an important role in contributing to the maintenance of international peace and security."*
	5.8 Internet	Pg. 9	*"Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet."*

	5.9 Election infrastructure	Pg. 9	*"Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet."*
	5.10 Harmful hidden functions	Pg. 11 para 58	*"To prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors, States can consider putting in place at the national level:..."*
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***		

xxxiii. UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015)

Agreement Overview			
I. Name of Agreement	**Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Report (2015)**		
II. Date it was signed/launched	**July 2015**	**III. Link**	**www.un.org/ga/search/view_doc.asp?symbol=A/70/174**
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**193**
VI. Organization responsible for ongoing	**United Nations**		

management of agreement (if any)			
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Sec. III (e)	*“Norms, rules and principles for the responsible behaviour of States* *States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;”*
		Sec. VI (26)	*In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.*
		Sec. VI (28b)	*“b) In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their*

			obligations under international law to respect and protect human rights and fundamental freedoms;"
	1.2 Personal data	Sec. 16 (d) (i)	*"(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:* *(i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;"* **NOTE: This is the only section 16 that cites data, but it does not exclusively cite 'personal data'.**
2. Information security and resilience measures	**2.1 CIP** (Critical Infrastructure Protection)	Sec. II (5) Sec. III (13) (f)	*"5. The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious."* *"(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;"*
	2.2 Essential services	Sec. III (13) (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;"*
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	

	2.5 Computer emergency response	Sec. IV (17) (c) (d) V (21) (a)	*"17. States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to: …* *(c) Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;* *(d) Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;"* *"21. Continuing the work begun through previous United Nations resolutions and reports, including General Assembly resolution 64/211, entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures", States should consider the following voluntary measures to provide technical and other assistance to build capacity in securing ICTs in countries requiring and requesting assistance:* *(a) Assist in strengthening cooperative mechanisms with national computer emergency response teams and other authorized bodies;"*
	2.6 Incident mitigation	Sec. III (13) (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;”
		Sec. IV (17) (a) (d) (e)	*“17. States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to:* *(a) Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;* *(d) Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;* *(e) Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.”*
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	Sec. III (13) (i)	*“(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;”*

	3.2 Reporting of vulnerabilities	Sec. III (13) (j) Sec. IV (16) (c) (d)	*"(j) States should encourage responsible reporting 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;"* *"(c) Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;* *(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders."*
4. Cooperation and assistance	**4.1 General cooperation**	Sec. III (9-15)	*"9. The ICT environment offers both opportunities and challenges to the international community in determining how norms, rules and principles can apply to State conduct of ICT-related activities. One objective is to identify further voluntary, non-binding norms for responsible State behaviour and to strengthen common understandings to increase stability and security in the global ICT environment.* *10. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and*

			intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development. *11. Previous reports of the Group reflected an emerging consensus on responsible State behaviour in the security and use of ICTs derived from existing international norms and commitments. The task before the present Group was to continue to study, with a view to promoting common understandings, norms of responsible State behaviour, determine where existing norms may be formulated for application to the ICT environment, encourage greater acceptance of norms and identify where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed.* *12. The Group noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an international code of conduct for information security (see A/69/723).* *13. Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:* *(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;* *(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; *(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;* *(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;* *(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;* *(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;* *(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;* *(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; *(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;* *(j) States should encourage responsible reporting 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;* *(k) States should not conduct or 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.* *14. The Group observed that, while such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity.* *15. Given the unique attributes of ICTs, additional norms could be developed over time."*
	4.2 Law enforcement assistance	Sec. III (10)	*"10. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT*

			environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.”
		Sec. III (13) (f)	*“(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;”*
		Sec. IV (16) (d) (i)	*“(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:* *(i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;”*
		Sec. IV (17) (a)	*“17. States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to:* *(a) Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;”*
			“(e) Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.”

		Sec. IV (17) (e) Sec. VI (24-29)	*“How international law applies to the use of ICTs* *24. The 2013 report stated that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. Pursuant to its mandate, the present Group considered how international law applies to the use of ICTs by States.* *25. The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.* *26. In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.* *27. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.* *28. Building on the work of the previous Groups, and guided by the Charter and the mandate contained in General Assembly resolution*

			68/243, the present Group offers the following non-exhaustive views on how international law applies to the use of ICTs by States: *(a) States have jurisdiction over the ICT infrastructure located within their territory;* *(b) In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;* *(c) Underscoring the aspirations of the international community to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter applies in its entirety, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group recognized the need for further study on this matter;* *(d) The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;* *(e) States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts;* *(f) States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State.*

			The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated. *29. The Group noted that common understandings on how international law applies to State use of ICTs are important for promoting an open, secure, stable, accessible and peaceful ICT environment."*
		Sec. VII (33-34)	*"33. The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States and developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour. Further work could consider initiatives for international dialogue and exchange on ICT security issues. These efforts should not duplicate ongoing work by other international organizations and forums addressing issues such as criminal and terrorist use of ICTs, human rights and Internet governance.* *34. The Group noted the importance of the consideration by the General Assembly of the convening of a new Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2016 to continue to study, with a view to promoting common understandings on existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as how international law applies to the use of ICTs by States, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building."*
	4.3 CIP assistance	Sec. II (5) (6)	*"II. Existing and emerging threats* *5. The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious.*

			6. The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security."
		Sec. III (13) (f) (g) (h) (j)	*"(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;* *(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;* *(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; …* *(j) States should encourage responsible reporting 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;"*
		Sec. IV (16)	*"16. Confidence-building measures strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability. In their work to build confidence to ensure a peaceful ICT environment, States should take into consideration the Guidelines for Confidence-building Measures adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78 (H). To enhance trust and*

			cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures:… *(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:* *(i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;* *(ii) The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;"*
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	Sec. III (3) (4)	*"3. ICTs provide immense opportunities for social and economic development and continue to grow in importance for the international community. There are, however, disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States, and the misuse of ICTs may harm international peace and security.* *4. A number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely."*
	5.2 Intellectual property	N/A	

	5.3 Non-proliferation	Sec. III (13) (i)	*"(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;"*
	5.4 Non-state actors	Sec. III (6) (7)	*"6. The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.* *7. The diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy."*
	5.5 Botnets	N/A	
	5.6 CIP	Sec. III (13) (f) Sec. IV (16) (d) (i) (ii)	*"(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;"* *"16. Confidence-building measures strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability. In their work to build confidence to ensure a peaceful ICT environment, States should take into consideration the Guidelines for Confidence-building Measures adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78 (H). To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures:*

			(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include: *(i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;* *(ii) The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;"*
	5.7 CERTs/CSIRTs	Sec. III (13) (k) Sec. IV (17) (c) (d)	*(k) States should not conduct or 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.* *(c) Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;* *(d) Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling*

			of ICT-related incidents and enhancing regional and sector-based cooperation
	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	Sec. V (21) (d)	*(d) Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance;*

xxxiv. UN Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021)

Agreement Overview			
I. Name of Agreement	Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (2021).		
II. Date it was signed/launched	**March 12, 2021**	**III. Link**	**https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf**
IV. Stakeholder groups party to the agreement	**Governments**	**V. Total Signatories/supporters**	**193**
VI. Organization responsible for ongoing management of agreement (if any)	**International Organization: United Nations**		
Norms Analysis			

Category	Norms elements	Paragraph /citation	Quote from Text
1. Rights and freedoms	**1.1 Human Rights**	Para. 15	*"States concluded that they are increasingly concerned about the implications of the malicious use of ICTs for the maintenance of international peace and security, and subsequently for human rights and development. In particular, concern was expressed regarding the development of ICT capabilities for purposes that undermine international peace and security. Harmful ICT incidents are increasing in frequency and sophistication and are constantly evolving and diversifying. Increasing connectivity and reliance on ICTs without accompanying measures to ensure ICT security can bring unintended risks, making societies more vulnerable to malicious ICT activities. Despite the invaluable benefits of ICTs for humanity, their malicious use can have significant and far-reaching negative impacts."*
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1 CIP (Critical Infrastructure Protection)**	Para. 31	*"States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore, States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection."*
	2.2 Essential services	Para. 26	*"While agreeing on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, along with endeavouring to ensure the general availability and integrity of the Internet, States further concluded that the COVID19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure. such as those affirmed by consensus through UN General Assembly resolution 70/237."*

	2.3 Electoral processes	Para. 18	*“States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. While it is each State’s prerogative to determine which infrastructures it designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation. Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability.”*
	2.4 Public trust		
	2.5 Computer emergency response	Para. 46	*“Drawing from the lessons and practices shared at the OEWG, States concluded that the prior existence of national and regional mechanisms and structures, as well as the building of adequate resources and capacities, such as national Computer Emergency Response Teams (CERTs), are essential to ensuring that CBMs serve their intended purpose.”*
	2.6 Incident mitigation	Para. 54	*“The international community’s ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. It is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. Capacity-building helps to develop the skills, human resources, policies, and institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies. It plays an important enabling function for promoting adherence to international law and the implementation*

			of norms of responsible State behaviour, as well as supporting the implementation of CBMs. In a digitally interdependent world, the benefits of capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all.”
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	Para. 28	*“States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities.”*
	3.2 Reporting of vulnerabilities	Para. 28	*“States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities.”*
4. Cooperation and assistance	**4.1 General cooperation**	Para. 55	*“Ensuring an open, secure, stable, accessible and peaceful ICT environment requires effective cooperation among States to reduce risks to international peace and security. Capacity-building is an important aspect of such cooperation and a voluntary act of both the donor and the recipient.”*
	4.2 Law enforcement assistance		
	4.3 CIP assistance	Para. 54	*“The international community’s ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State*

			to prepare and respond. It is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. Capacity-building helps to develop the skills, human resources, policies, and institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies. It plays an important enabling function for promoting adherence to international law and the implementation of norms of responsible State behaviour, as well as supporting the implementation of CBMs. In a digitally interdependent world, the benefits of capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all."
	4.4 Due diligence	Para. 31	*"States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore, States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection."*
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	Para. 16	*"States recalled that a number of States are developing ICT capabilities for military purposes. They also recalled that the use of ICTs in future conflicts between States is becoming more likely. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a*

			disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States."
	5.5 Botnets		
	5.6 CIP	Para. 31	*"States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore, States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection."*
	5.7 CERTs/CSIRTs	Para. 61	*"States recalled the need for a concrete, action-oriented approach to capacity-building. States concluded that such concrete measures could include support at both the policy and technical levels such as the development of national cyber security strategies, providing access to relevant technologies, support to Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) and establishing specialized training and tailored curricula including "training the trainer" programmes and professional certification. The benefits of establishing platforms for information exchange including legal and administrative good practices was recognized, as were the valuable contributions of other relevant stakeholders to capacity-building activities."*
	5.8 Internet	N/A	
	5.9 Election infrastructure	Para. 18	*"States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. While it is each State's prerogative to determine which infrastructures it designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation. Malicious ICT activities against CI and CII that undermine trust and*

			confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability."
	5.10 Harmful hidden functions	Para. 28	*"States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities."*
6. Technical/Operational	**6.1 Network Security Practices**		
Any other norms areas included?	***Description:***	Para. 41-47; Para. 54-56	Capacity Building, Confidence Building

xxxv. XII BRICS Summit Moscow Declaration

Agreement Overview			
I. Name of Agreement	**XII BRICS Summit Moscow Declaration**		
II. Date it was signed/launched	Nov. 17, 2020	**III. Link**	https://eng.brics-russia2020.ru/images/114/81/1148126.pdf
IV. Stakeholder groups party to the agreement	Governments	**V. Total Signatories/supporters**	5

VI. Organization responsible for ongoing management of agreement (if any)	BRICS		
Norms Analysis			
Category	**Norms elements**	**Paragraph/ citation**	**Quote from Text**
1. Rights and freedoms	**1.1 Human Rights**	Para 39	*“We emphasize the need of a comprehensive and balanced approach to ICTs development and security, including technical advancement, business development, of safeguarding the security of States and public interests, and of respecting the right to privacy of individuals.”*
	1.2 Personal data	N/A	
2. Information security and resilience measures	**2.1CIP**	N/A	
	2.2 Essential services	N/A	
	2.3 Electoral processes	N/A	
	2.4 Public trust	N/A	
	2.5 Computer emergency response	N/A	
	2.6 Incident mitigation	N/A	
	2.7 Cyber hygiene	N/A	
3. Reliability of products	**3.1 Supply chain**	N/A	
	3.2 Reporting of vulnerabilities	N/A	
4. Cooperation and assistance	**4.1 General cooperation**	Para. 40	*“We also underscore the importance of establishing legal frameworks of cooperation among BRICS States on ensuring security in the use of ICTs. We note the activities of the BRICS Working Group on Security in*

			the Use of ICTs and acknowledge the work towards consideration and elaboration of proposals on this matter, including on a BRICS intergovernmental agreement on cooperation on ensuring security in the use of ICTs and on bilateral agreements among BRICS countries."
	4.2 Law enforcement assistance	Para 41	*"While emphasizing the formidable potential of the digital revolution for growth and development, we recognize new associated possibilities it brings for criminal activities and threats. We express concern over the rising level and complexity of criminal misuse of ICTs as well as the absence of a multilateral framework to counter the use of ICTs for criminal purposes. We recognize also that new challenges and threats in this respect require international cooperation and discussions on possible legal frameworks, including the need to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes under the auspices of the UN and note the establishment of an openended ad hoc intergovernmental committee of experts under the auspices of the UN in accordance with UNGA Resolution 74/247 of 27 December 2019."*
	4.3 CIP assistance	N/A	
	4.4 Due diligence	N/A	
5. Restraint on development and use of cyber capabilities	**5.1 Developing and deploying cyber weapons**	N/A	
	5.2 Intellectual property	N/A	
	5.3 Non-proliferation	N/A	
	5.4 Non-state actors	N/A	
	5.5 Botnets	N/A	
	5.6 CIP	N/A	
	5.7 CERTs/CSIRTs	N/A	

	5.8 Internet	N/A	
	5.9 Election infrastructure	N/A	
	5.10 Harmful hidden functions	N/A	
6. Technical/Operational	**6.1 Network Security Practices**	N/A	
Any other norms areas included?	***Description:***		

Disclaimer:

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.